E.T.S. de Ingeniería Industrial,
Informática y de Telecomunicación

Efecto de la red en las prestaciones de escritorios en la nube

Grado en Ingeniería
en Tecnologías de Telecomunicación

Trabajo Fin de Grado

Autor: Javier Rubio Sanz

Director: Eduardo Magaña Lizarrondo

Pamplona, 23 de junio de 2016

upna Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Agradecimientos

En primer lugar, me gustaría agradecer tanto a VNC, como Microsoft y TeamViewer la posibilidad de utilizar su software para este análisis, además de la posibilidad de hacerlo gratuitamente.

En segundo lugar, agradecer a Eduardo por su incansable ayuda y sus necesarios consejos durante el desarrollo del proyecto, además de la posibilidad de realizar los análisis en un laboratorio de la universidad.

Por último y no menos importante, me gustaría agradecer a mi familia el esfuerzo que les supone que yo actualmente esté realizando este proyecto, a mis amigos por sus consejos y a todas las personas que tengo diariamente a mi alrededor que no se cansan de apoyarme.

Resumen

Debido a que muchos responsables de las tecnologías de la información están empezando a implementar algún tipo de entorno de trabajo virtual, Amazon Web Services ofrece un servicio de servidores totalmente gestionados en la nube, llamado Amazon Elastic Compute Cloud. Por ello, hemos realizado un análisis del funcionamiento de estos servidores en distintos perfiles de trabajo como son el ofimático, navegación y audiovisual. Para acceder al servidor hemos utilizado los siguientes protocolos: RDP, VNC, TeamViewer.

Además, entre el cliente y Amazon se ha colocado un equipo que haga de router NAT y de conformador de tráfico. Hemos elaborado un script limitador, mediante el paquete traffic control, “tc”, que ofrece Linux, para realizar un análisis más completo del escritorio remoto, y así establecer diferentes limitaciones a la red para observar cómo se comportan los distintos perfiles y sacar como conclusiones las limitaciones que tiene la funcionalidad de ambos servicios en diferentes entornos de trabajo y cuál será el mejor protocolo para estos entornos.

Índice

Índice de figuras

1. Introducción

La evolución de las comunicaciones tanto en el ámbito laboral como en el ámbito privado obliga a crear facilidades a los usuarios como la posibilidad de utilizar tu equipo de trabajo o del hogar desde cualquier punto con conexión a Internet. Por ello, sobre este proyecto, trataremos de analizar los efectos que puedan surgir en escritorios remotos gestionados en la nube, como limitaciones, latencias u otros efectos.

Sobre este planteamiento, analizaremos esos efectos sobre protocolos como son RDP [17], VNC [19], y sobre el software TeamViewer [20].

Los escritorios remotos gestionados en la nube serán los servidores que ofrece Amazon Web Services. [7].

Por tanto, para comenzar, explicaremos cada uno de los conceptos que aparecerán sobre el proyecto.

1.1. Sistemas de escritorio remoto

Como planteamiento de este proyecto, se ha profundizado sobre estos conceptos.

1.1.1. Escritorio remoto

Un servicio de escritorio remoto es una tecnología que permite a un usuario trabajar en un equipo informático a través de otro equipo informático situado en otro lugar [14]. Esta utilidad es muy común en técnicos informáticos que desean acceder al equipo del cliente y solucionar un problema al instante. También es común en trabajadores, que desde su vivienda, desean acceder a su ordenador de trabajo y hacer las gestiones pertinentes sobre él. Actualmente, es una tecnología muy utilizada, incluso en dispositivos móviles.

Existen varios protocolos encargados de la conexión remota, entre los que destacan RDP, VNC, X11 o ARD.

1.1.2. RDP - Remote Desktop Protocol

RDP (Remote Desktop Protocol) [17] es un protocolo utilizado en el escritorio remoto de Windows, cuyo propietario es Microsoft. Este protocolo emplea el puerto TCP 3389. Sobre TCP, va un protocolo especial, llamado TPKT, el cual se define como “Servicio de Transporte ISO en la parte superior de TCP”. [15].

La conexión a un servidor gestionado en la nube sobre este protocolo garantiza buenos resultados, porque RDP conoce las primitivas graficas al procesar una imagen de pantalla a través de la red, entonces aprovecha esa información para comprimir el flujo de datos notablemente. Es decir, si un trozo de la pantalla está ocupado por un conjunto de tonos verdes, el protocolo no enviará toda la imagen de la pantalla sino que solo enviará la ubicación de esos tonos, el tamaño o el color de éstos.

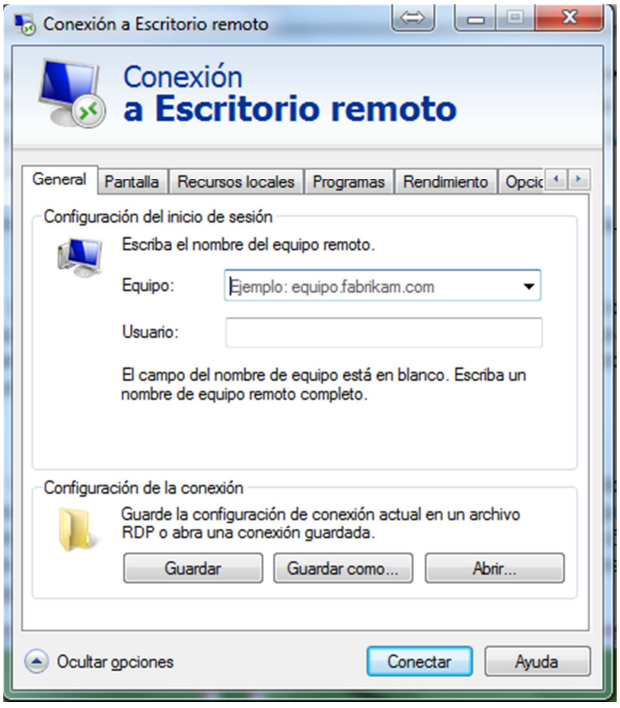

Figura 1.1. Cliente escritorio remoto de Windows

RDP tiene como características principales:

- Colores de 8, 16, 24 y 32 bits.
- Cifrado de 128 bits.
- Seguridad a nivel de transporte.

- Ancho de banda ajustado para clientes RDP.

Como ventajas, este protocolo tiene el almacenamiento de caché, ya que el cliente puede almacenar gran cantidad de información del servidor al que se ha conectado, para que si volviese a establecerse esa conexión, la información obtenida en la primera conexión será válida para las siguientes conexiones. Además, RDP puede transmitir audio.

Como desventajas, este protocolo solo puede ser utilizado en sistemas operativos de Microsoft y no está disponible la transferencia de archivos entre el cliente y el servidor.

1.1.3. VNC - Virtual Network Computing

VNC (Virtual Network Computing) [19] es una alternativa a lo que ofrece Microsoft. Además, VNC es independiente de la plataforma y compatible con cualquier sistema operativo. VNC se desarrolló en los laboratorios de AT & T. Su código fuente es código abierto bajo la licencia GNU (General Public License). Tiene proyectos derivados como RealVNC o UltraVNC. En este proyecto utilizaremos el primero, RealVNC, el cual lo hemos obtenido desde su página oficial https://www.realvnc.com/.

Este protocolo requiere la apertura de los puertos TCP 5800 y 5900. Sobre esta conexión, se utiliza un protocolo llamado RFB (Remote Framebuffer), el cual es un protocolo mejorado sobre TCP, que permite la transferencia de archivos y técnicas de seguridad y compresión más sofisticadas.

El propio servidor VNC ofrece diferentes opciones como seguridad, usuarios y permisos, conexiones, privacidad, actualizaciones, etc., y un nivel más avanzado de modificaciones del software. El cliente, en este caso VNC Viewer, ofrece más opciones sobre la calidad de visualización del escritorio remoto al que se quiere conectar.

Además, VNC a diferencia de RDP, este protocolo no es tan inteligente en conocer las primitivas gráficas de la imagen, por lo que VNC tiene técnicas de

compresión más básicas. Envía los bloques de mapa de bits que han cambiado y utiliza tipos de compresión como RLE [21] o JPEG [22].

Respecto a este protocolo, podemos hablar de varios factores como la velocidad de conexión, la latencia o el uso de la red.

- **Velocidad de conexión**

VNC se ajusta a cualquier conexión a Internet. Cuanto más lenta la conexión, peor calidad de imagen. Generalmente las conexiones más lentas son recomendables sólo para trabajar con documentos o pequeñas aplicaciones. Para trabajar imágenes y video en alta calidad, se requiere un ancho de banda mayor.

- **Latencia**

Latencia refiere al retardo en la comunicación entre dos dispositivos. Incluso teniendo una conexión de ancho de banda grande, puede haber rendimiento lento en VNC si estás lejos del ordenador al que se desea acceder. Esto es principalmente un problema para los usuarios a miles de kilómetros de distancia.

- **Uso de la red**

También se debe tener en cuenta el uso de la red. Si se comparte una conexión con varios usuarios o descargando archivos durante el uso de VNC, el rendimiento se verá afectado. [16].

Como ventajas, como hemos comentado anteriormente, VNC permite la transferencia de ficheros y se puede utilizar en cualquier sistema operativo.
Como desventajas, no es capaz de transmitir audio, y su forma de compresión no es eficaz, respecto a RDP.

1.1.4. TeamViewer

TeamViewer [20] es un software que permite la conexión y control de un escritorio remoto. Actualmente es propiedad de GFI Software y, como VNC, es compatible para cualquier sistema operativo. Sus funciones se basan en

compartir y controlar escritorios, videoconferencias, transferencias de ficheros, etc., pero el principal uso de este software es el acceso a un equipo remoto.

Figura 1.2. TeamViewer

El funcionamiento de este software es muy sencillo. Simplemente es necesario tener conexión a internet tanto en el cliente como en el equipo remoto y conocer del equipo remoto su ID y contraseña para poder acceder a él. Una vez accedes al equipo, tanto el cliente como el equipo remoto se mandan paquetes UDP entre ellos cada pocos segundos. Si esa conexión se realiza en una red local, la conexión entre ambos es directa. Si la conexión es a través de Internet, los paquetes que son intercambiados pasan por un servidor central de TeamViewer.

Como ventajas, TeamViewer ofrece compatibilidad con diferentes sistemas operativos, facilidad de uso, seguridad de conexión o transferencia de ficheros. TeamViewer incluye cifrado basado en el intercambio de claves públicas/privadas RSA 2048 y cifrado de sesión AES (256 bits). Esta tecnología se basa en los mismos estándares que https/SSL y cumple los estándares actuales de seguridad. [20]. Como desventajas, es un protocolo propietario y existe un retardo notable debido a su baja tasa de transmisión. [18].

1.1.5. AWS – Amazon Web Services

AWS [7] es una plataforma de servicios gestionados en la nube que ofrece variedad de productos como almacenamiento de bases de datos, servidores o escritorios remotos gestionados en la nube. AWS proporciona una gran colección de servicios de infraestructura.

Esta plataforma tiene como características principales su seguridad, su bajo coste o su flexibilidad al lenguaje o sistema operativo del cliente.

Entre los servicios que ofrece AWS, destacamos:

- ✓ Escritorio remoto gestionado en la nube.
- ✓ Servidores gestionados en la nube.
- ✓ Servicio de E-mail y calendario.
- ✓ Bases de datos.
- ✓ Almacenamiento en la nube.
- ✓ Redes privadas virtuales.
- ✓ Etc.

Sobre este proyecto, nos centraremos en analizar los efectos de la red en los servidores que proporciona Amazon.

1.1.5.1. Amazon Elastic Compute Cloud – EC2

Servicio que proporciona la posibilidad de hospedar servidores virtuales, con características modificables de almacenamiento, memoria o CPU. Amazon EC2 presenta un entorno virtual con instancias que permiten utilizar distintos sistemas operativos. Esas instancias, como se comenta en el apartado 2.3.1, son instancias de diferentes tamaños, con mejores y peores prestaciones y diferentes precios para el cliente, a elección de sus necesidades.

2. Configuración del entorno

Pudiendo hacer un análisis más completo del rendimiento de los servicios que ofrece Amazon, se establece entre el servicio y el cliente un equipo que haga como router, el cual se configura tal que realice funciones de conformador de tráfico que establezca o no limitaciones en la red.

Como características principales de ese equipo, tendrá que incorporar dos tarjetas de red, una que esté directamente conectada a Internet y la otra esté conectada a una red local donde esté el cliente.

Además, en el interfaz que esté directamente conectado a Internet, activaremos el mecanismo NAT para que el cliente pueda enviar y recibir paquetes procedentes de Internet aun teniendo una red interna con direccionamiento privado. Para ello, en el equipo configurado como router también habrá que activar el enrutamiento de paquetes. Estos pasos mencionados serán explicados posteriormente.

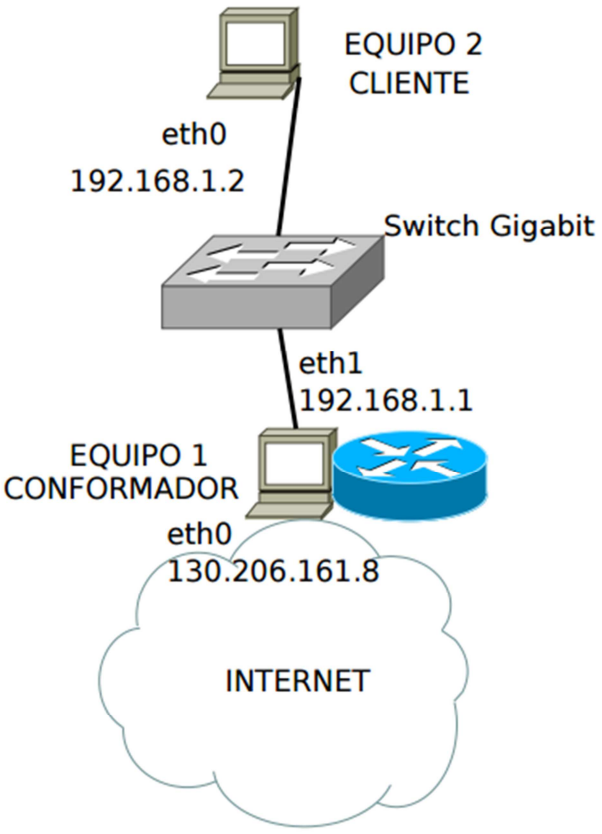

Figura 2.1. Red del entorno

2.1. Configuración del equipo conformador

El interfaz eth0, inicialmente estaba conectado al NAT del laboratorio, pero para evitar posibles efectos de éste, lo hemos conectado directamente a internet con una IP pública 130.206.161.8/20. El interfaz eth1, conectado a una red local con direccionamiento IP de clase C (privado), estará conectado a la red 192.168.1.0/24.

Como cada vez que reiniciamos el equipo, el interfaz conectado a la red local pierde su direccionamiento IP, asignamos una configuración fija para no tener que volver a ser configurado.

Entonces seguimos los siguientes pasos: [1]

1. Abrimos un terminal y accedemos al siguiente fichero de configuración:

   sudo nano /etc/network/interfaces

2. En el fichero abierto escribimos los siguientes comandos:

   auto eth1

   iface eth1 inet static

   address 192.168.1.1

   netmask 255.255.255.0

3. Así ya tendremos una IP fija en el interfaz conectado a la red LAN, en este caso eth1.

También se necesita que el equipo tenga el mecanismo de NAT activado, por tanto debemos seguir los siguientes pasos: [2]

1. En terminal, accedemos a modificar el siguiente fichero del equipo:

   sudo /etc/rc.local

2. Incluimos las siguientes líneas en el fichero:

   echo 1 > /proc/sys/net/ipv4/ip_forward

   ##Modifica el fichero a 1 para activar el enrutamiento
   iptables –t nat –A POSTROUTING –o eth0 -j MASQUERADE

##Activa el Nat del equipo para que los paquetes de la red local salgan con IP pública al exterior
iptables –A FORWARD –i eth1 -j ACCEPT

##Acepta todos los paquetes que vienen del exterior convertidos de IP pública a IP privada

3. Guardamos y cada vez que reiniciemos el equipo ya tendrá el NAT activado.

2.1.1. Equipo como conformador de tráfico

2.1.1.1. Hardware del equipo

- Procesador: Intel® Core™2 Quad CPU Q9400 @ 2.66 GHz
- Memoria: 3.5 GB
- Kernel: Linux 3.19.0-25-generic(x86.64)
- Disco duro: 250 GB
- Versión Ubuntu: Ubuntu 14.04.4 LTS

2.1.1.2. Conformador de tráfico

Un sistema de conformación de tráfico permite adecuar el tráfico de datos entrante dándole un tratamiento especial llamado *traffic shaping* o conformación de tráfico aceptado, y que permita que algunas de las tramas puedan ser rechazadas, duplicadas o enviadas más tarde, con un retardo añadido.

En este análisis se pretende utilizar un conformador de tráfico para ver qué rendimiento necesitan diferentes perfiles de uso de un escritorio remoto con distintas limitaciones de ancho de banda.

En este caso se utilizará un *traffic control* de máquinas Ubuntu en el que se configura a través del terminal mediante comandos con “tc”. [4]
Mediante ese comando se puede establecer diferentes prioridades para los paquetes para filtrarlos y clasificarlos en mayor o menor importancia.
Para poder trabajar con ese paquete de comandos se necesita tener instalado el paquete iproute en nuestra máquina que vaya a funcionar como conformadora de tráfico. Por tanto, desde el terminal, se ejecutará el siguiente comando:

sudo apt-get install iproute

Si por ejemplo se quiere añadir un retardo a la red se utiliza un emulador de red incorporado en el paquete instalado, llamado NetEm (Emulador de red). Para ejecutarlo se pondría un comando de estas características:

sudo tc qdisc add dev eth1 root netem delay 250ms

donde en eth1 sería el interfaz dónde se quiere configurar el retardo y el *delay* sería el retardo que se desee. [5].

Además, el emulador de red también permite añadir otros efectos en la red como la pérdida de paquetes (*loss*), en el cual se establece un porcentaje de paquetes perdidos, o hacer un duplicado de paquetes (*duplicate*), donde también se establece un porcentaje de paquetes duplicados. Todas estas opciones son aplicadas tanto en el tráfico de subida como en el tráfico de bajada.

Para eliminar la configuración establecida habría que ejecutar el siguiente comando:

sudo tc qdisc del dev eth1 root netem

Para limitar las conexiones de ancho de banda de la red creado un script [Anexo 3], el cual utiliza opciones que incorpora el paquete instalado anteriormente. [6].

Para ejecutarlo, habrá que poner lo siguiente en terminal:

sudo sh shaper.sh start eth1 5000

Donde el primer parámetro será que deseamos hacer (start, stop o status), el siguiente parámetro será el interfaz donde queremos aplicar la limitación y, por último, el tercer parámetro será la velocidad a la que queremos limitar el interfaz.

Si deseamos eliminar la configuración, simplemente se pondrá lo siguiente:

sudo sh shaper.sh stop eth1

Si deseamos observar la configuración que tiene el controlador de tráfico habrá que escribir lo siguiente:

sudo sh shaper.sh status eth1

El tráfico limitado será capturado para un posterior análisis en el interfaz eth0 del equipo conformador, para ver el tráfico conformado tanto de subida como de bajada.

2.2. Configuración del equipo cliente

Este equipo será desde el que realicemos el análisis de los escritorios remotos y tendrá una única tarjeta de red conectada a la red local con direccionamiento IP de clase C en la red 192.168.1.0/24 que se unirá al equipo conformador a través de un Switch Gigabit Ethernet mediante un cable de par trenzado.

Como nos ocurre en el equipo conformador, debemos asignarle una IP fija al interfaz para que, en caso de reinicio del equipo, no se borre el direccionamiento IP.

Seguimos los siguientes pasos:

1. Abrimos un terminal y accedemos al siguiente fichero de configuración:

   sudo nano /etc/network/interfaces

2. En el fichero abierto escribimos los siguientes comandos:

   auto eth0

   iface eth0 inet static

   address 192.168.1.2

   netmask 255.255.255.0

   gateway 192.168.1.1

   dns-nameservers 10.1.1.193

Básicamente lo que hacemos es darle de forma estática una IP, una máscara, su puerta de enlace al conformador y la dirección del servidor DNS para poder conectarse a direcciones IP con DNS.

3. Así podemos comprobar como ya tenemos conexión a Internet. [3]

2.2.1. Equipo Cliente

Este equipo está configurado con un arranque dual, que permita iniciar sesión tanto con el sistema operativo Linux, como Windows.

2.2.1.1. Hardware del equipo

- Procesador: Intel® Core™2 Duo CPU E6750 @ 2.66 GHz
- Memoria: 4 GB
- Kernel: Linux 3.19.0-25-generic(x86.64)
    - Disco duro: 50 GB
    - Versión Ubuntu: Ubuntu 14.04.4 LTS
- Edición: Windows 7 Professional
    - Tipo de sistema: Sistema operativo de 64 bits
    - Disco duro: 200 GB

2.3. Servidor Amazon EC2

Amazon proporciona una gran selección de instancias para diferentes usos. Además, ofrece diferentes variedades de instancias para varias combinaciones de capacidad de CPU, memoria, almacenamiento y redes. Para este proyecto, vamos a analizar los efectos de la red con una instancia de las que ofrece el servicio de Amazon gratuitamente para estudiantes. [7]. La capa gratuita proporciona una instancia T2 micro, que es una instancia de desempeño a ráfagas, es decir, para un uso de la CPU por encima del nivel básico y muy de vez en cuando alcanzan ráfagas más altas llegando a usar la CPU por completo. Como característica, la instancia T2 micro tiene:

- Procesador Intel Xeon de alta frecuencia con Turbo hasta 3,3 GHz
- CPU en ráfagas, que se basa en créditos de CPU, que se acumulan cuando el servidor está desconectado. (6 créditos por hora)
- Equilibrio entre recursos de informática, memoria y red. (1 GB de memoria).

Ahora se procederá a explicar cómo crear un servidor gestionado en la nube.

2.3.1. Instances

Para poder obtener nuestra propia instancia, primero hay que crearnos una cuenta en Amazon Web Services. Para recibir créditos gratuitos y ser gastados en diferentes servicios que ofrece Amazon, es necesario acudir a la web: http://aws.amazon.com/es/education/awseducate/, crear una cuenta con el correo de la universidad donde se está estudiando, y así obtener 100 $ introduciendo un código promocional recibido, en nuestro apartado de créditos de la cuenta personal.

Por tanto, procedemos a crear la instancia. Para ello, accedemos a la consola de AWS (Amazon Web Services), como se puede observar en la imagen posterior:

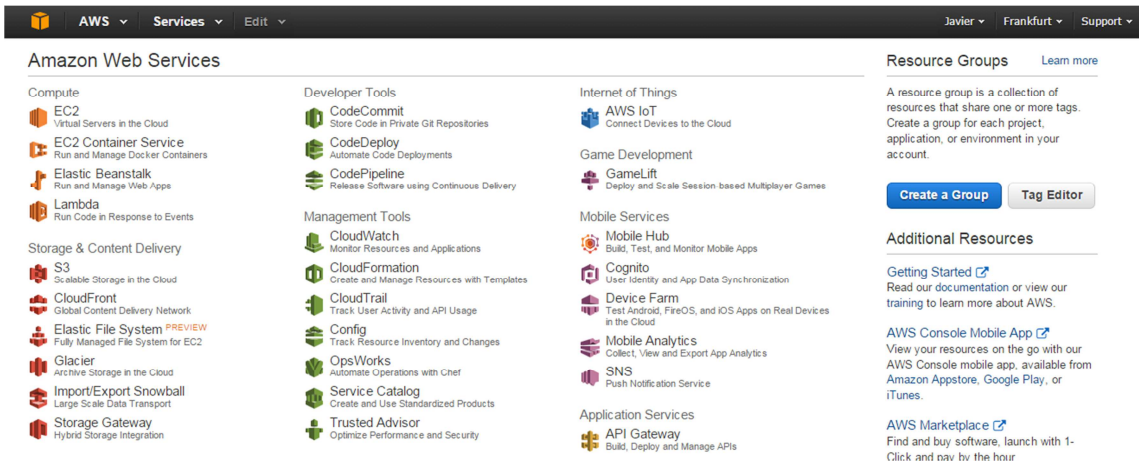

Figura 2.2. Consola de AWS

Después accedemos al enlace EC2, donde se encontrarán todas las configuraciones que haremos a continuación. Una vez pulsado, clickamos sobre el botón azul que pone "*Launch instance*", para acceder a la elección de la instancia en la siguiente ventana.

Aquí podemos seleccionar el tipo de máquina que se quiere ejecutar con el sistema operativo que se desee. Para ello, previamente pulsamos la pestaña que hay a la izquierda de los servidores, donde pone "*Free tier only*", para saber cuáles son los servidores que ofrece Amazon en versión gratuita. Escogemos el que queremos pulsando "*Select*".

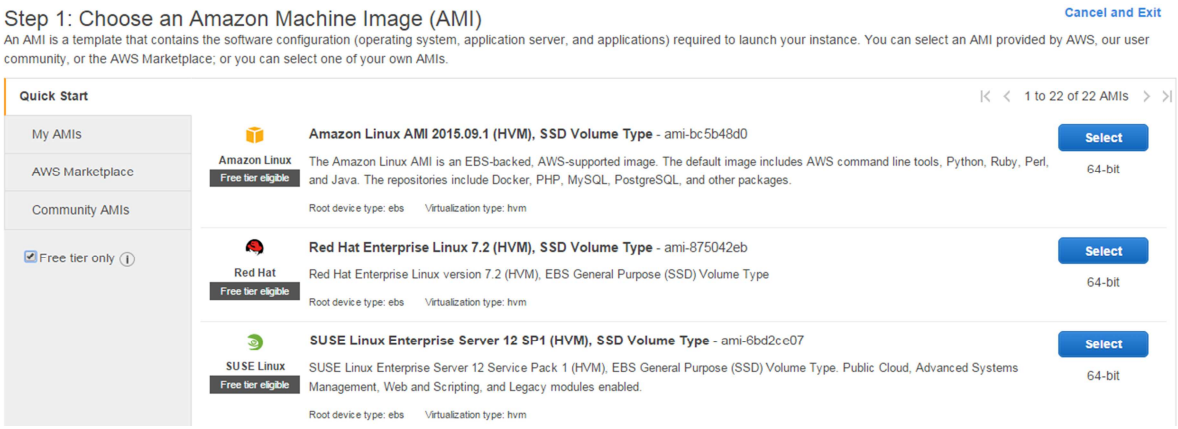

Figura 2.3. Elección del servidor.

Una vez seleccionado, nos aparece una ventana donde se debe elegir el tipo de instancia que se quiere y, como anteriormente hemos hecho, escogemos la instancia que nos proporcionan como "*Free tier eligible*" y pulsamos "*Review and Launch*".

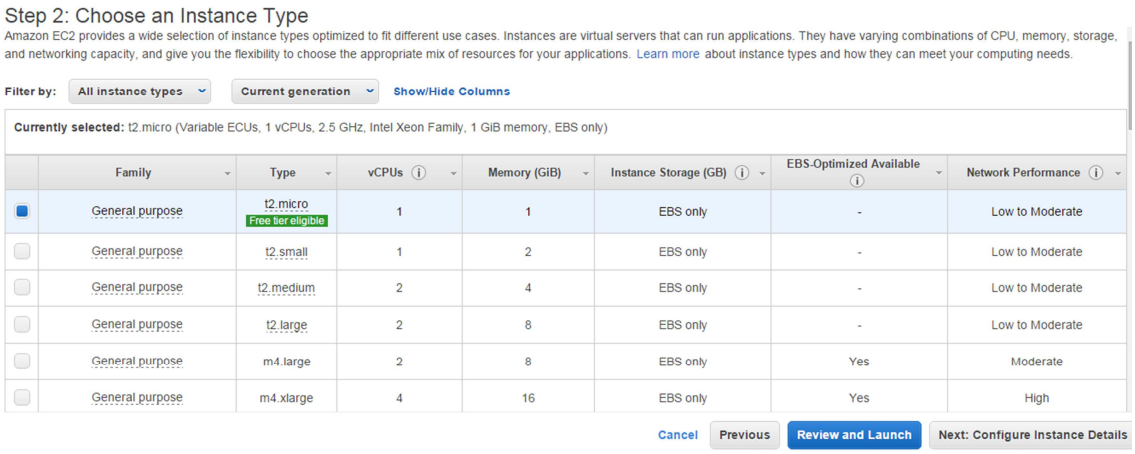

Figura 2.4. Elección del tipo de instancia

En la siguiente ventana pulsamos sobre "*Launch*" y nos aparecerá una ventana donde crearemos las claves para, posteriormente, poder acceder a nuestro servidor gestionado en la nube. Para ello, en la pestaña "*Choose an existing key pair*", seleccionamos "*Create a new key pair*", le damos un nombre a la clave y pulsamos "*Download Key Pair*".

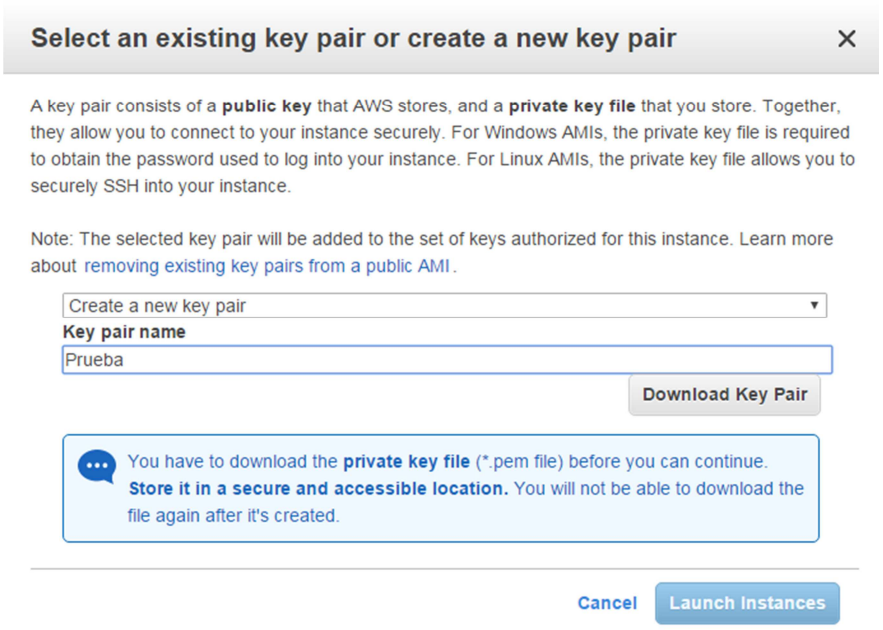

Figura 2.5. Creación de las claves de acceso

Una vez descargada la clave, pulsamos sobre "*Launch Instances*" y ya tenemos creada nuestra instancia donde trabajaremos con los protocolos RDP y VNC. La podemos ver pulsando sobre "*View Instances*".

Para conectarse a la instancia, pulsamos sobre ella, le damos al botón "*Connect*" y en la siguiente ventana tendremos que generar una contraseña pulsando en "*Get Password*" y buscando las claves descargadas anteriormente. Una vez abierto el archivo de claves, desencriptamos la clave pulsando en "*Decrypt Password*". Así ya tenemos nuestra contraseña preparada. Para acceder al servidor en la nube, lo haremos de dos formas distintas:

- Mediante el protocolo RDP.

Si utilizamos en el cliente como sistema operativo, Linux, utilizaremos el Cliente de escritorio remoto Remmina, que viene instalado. Para ello se debe poner como Host la DNS pública de la instancia, por ejemplo: ec2-52-58-77-85.eu-central-1.compute.amazonaws.com, que la podemos encontrar en la siguiente información:

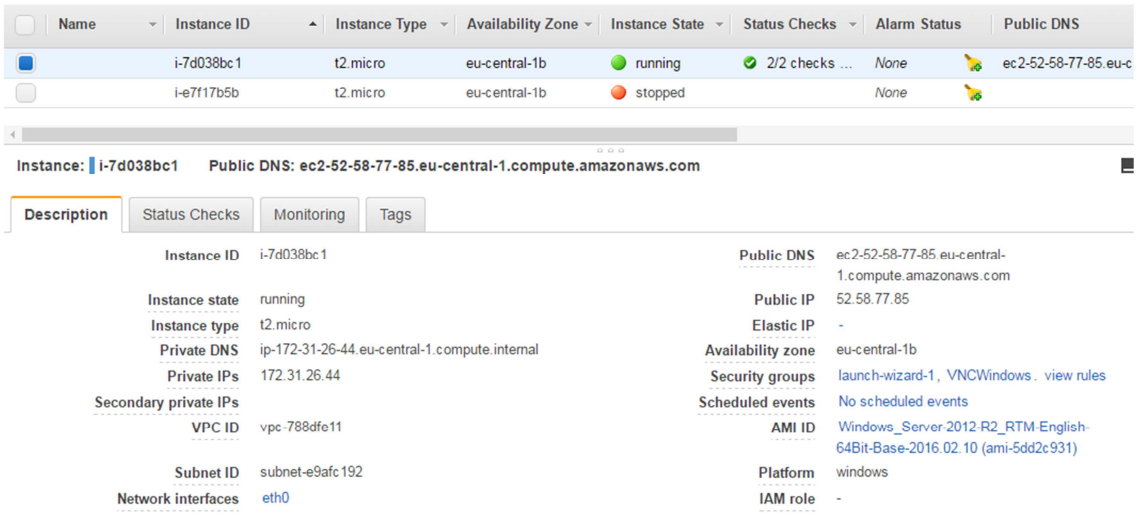

Figura 2.6. Descripción del servidor

El usuario será "*Administrator*" y la contraseña, la adquirida anteriormente. Conectamos y aparecerá nuestro servidor en la nube listo para ser utilizado.

Si utilizamos el cliente como sistema operativo Windows, simplemente se pulsará la pestaña "*Download Remote Desktop File*", lo ejecutamos y le introducimos la contraseña.

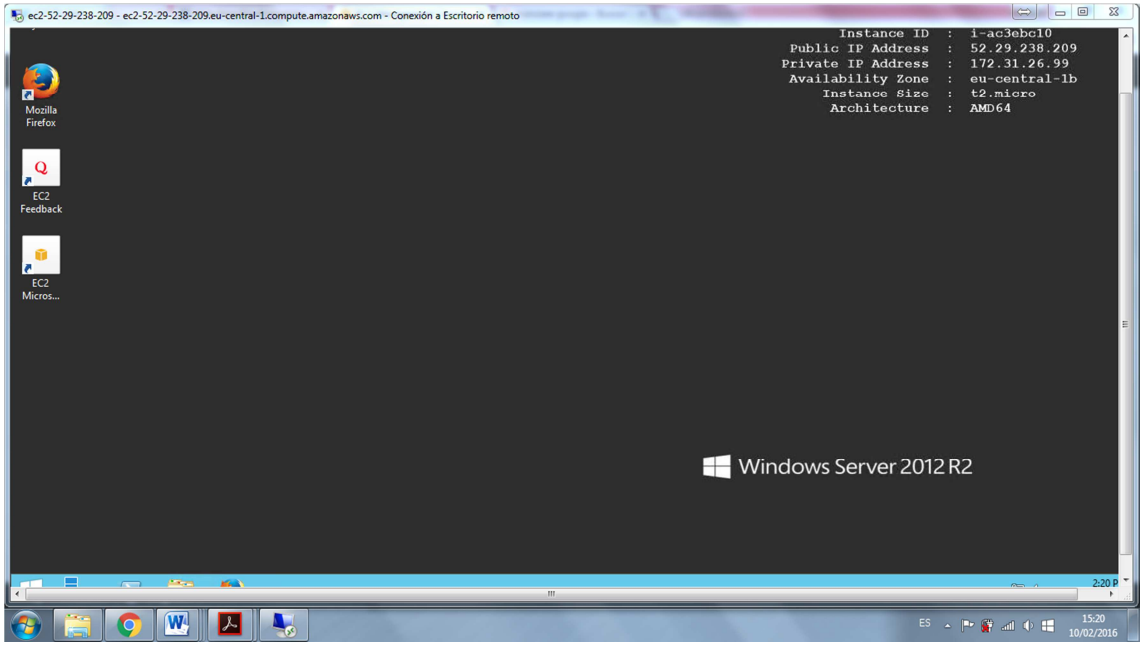

Figura 2.7. Servidor en la nube.

- Mediante el protocolo VNC.

Mediante este protocolo, necesitamos tener un servidor VNC en funcionamiento en el servidor en la nube. Por ello, hemos instalado RealVNC sobre él y accedemos al escritorio remoto mediante un cliente de RealVNC desde nuestro equipo cliente Linux. Para acceder a él escribimos sobre la dirección del cliente RealVNC la dirección pública de nuestro servidor, por ejemplo: 52.58.77.85 o ec2-52-58-77-85.eu-central-1.compute.amazonaws.com y accedemos a conectarnos. Para acceder completamente a nuestro servidor, nos pedirá un usuario y una contraseña, que serán los mismos que los utilizados en el protocolo RDP.

Para poder acceder a nuestro servidor, antes debemos configurar los puertos TCP abiertos 5800 y 5900, puertos utilizados por VNC, que se hace desde otro servicio que ofrece Amazon EC2, los "*Security Groups*". Para el protocolo RDP, el servicio de Amazon ya crea automáticamente el grupo de seguridad para el puerto TCP 3389 al crear el servidor.

- Mediante TeamViewer

Descargamos el servidor de TeamViewer de su página oficial https://www.teamviewer.com/es/, lo instalamos y sobre él, podemos crear una cuenta para guardar el equipo servidor con su respectiva ID y su contraseña. Una vez guardado el servidor, solamente deberemos ejecutar en el cliente TeamViewer, iniciar sesión en nuestra cuenta creada y conectarnos al servidor ya almacenado pulsando doble click sobre él. En este caso no se es necesario abrir ningún puerto de seguridad.

2.3.2. Security Groups

Un grupo de seguridad actúa como un Firewall virtual que controla el tráfico para una o más instancias. Cuando se crea una instancia, se le debe asignar uno o varios grupos de seguridad.

En este proyecto, lo necesitamos para abrir los puertos mencionados anteriormente y que podamos acceder al servidor en la nube mediante el protocolo VNC.

Por ello, vamos a explicar cómo crear un grupo de seguridad y como asignárselo a una instancia.

Nos situamos en la ventana de Amazon EC2 y en el menú de la izquierda, donde pone "*Network & Security*" accedemos a "*Security Groups*".

Pulsamos sobre el botón azul "Create Security Group" y nos aparece la siguiente ventana:

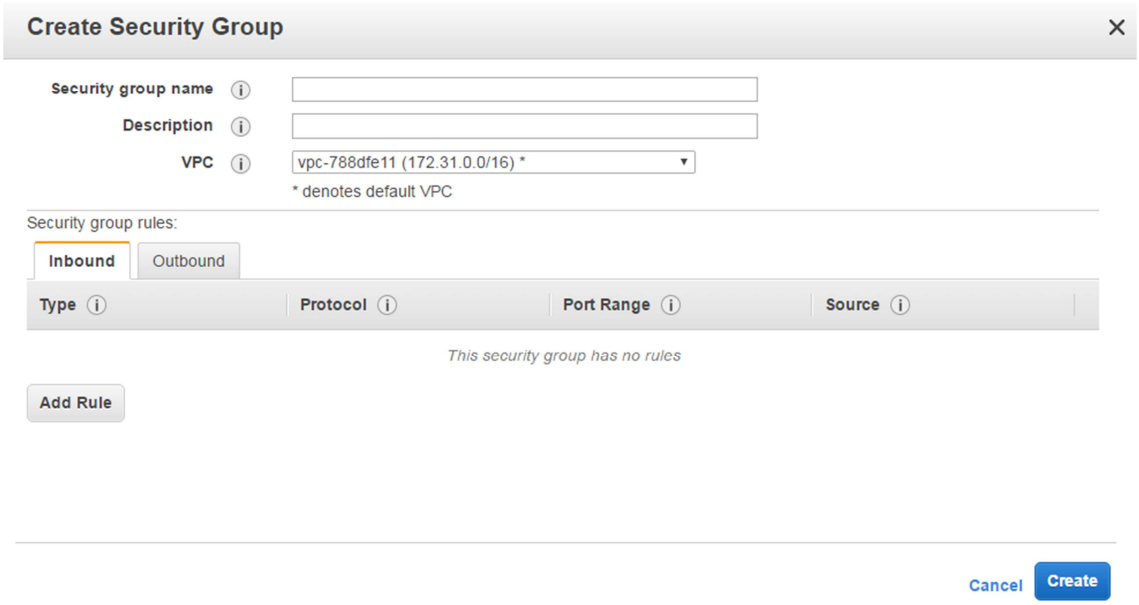

Figura 2.8. Creación Security Group

En ella, podemos asignarle un nombre y una descripción. Debajo, en "*Inbound*" añadimos una nueva regla:

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	5900	0.0.0.0/0
Custom TCP Rule	TCP	5800	0.0.0.0/0

Figura 2.9. Asignación de las reglas en el Security Group

Finalmente, pulsamos "*Create*" y ya tenemos nuestro grupo de seguridad creado. Solo nos falta asignarle a nuestra instancia este grupo de seguridad.

Para ello vamos donde se encuentran las instancias pulsando en "*Instances*" del menú de la izquierda. Hacemos click derecho sobre nuestra instancia, nos situamos sobre la pestaña "*Networking*" y accedemos a su submenú para acabar pulsando en "*Change Security Groups*". Una vez pulsado, accedemos a

la ventana donde podremos seleccionar el grupo de seguridad creado. Así, ya tendremos el puerto abierto y podremos acceder mediante un servidor VNC a nuestra instancia.

2.3.3. Creación de macros

Debido a las numerosas pruebas que vamos a hacer en diferentes servicios y con diferentes protocolos, para agilizar los análisis, vamos a generar diferentes macros de pulsaciones de teclado y ratón para que se ejecute una grabación realizada anteriormente en la que haga diferentes movimientos en el escritorio remoto. El software que se ha utilizado ha sido Macro Recorder. [8].

Con motivo de hacer un análisis más completo del escritorio remoto hemos dividido las grabaciones de macros en tres perfiles distintos, aunque existirá en el posterior análisis un cuarto perfil de inicio de sesión al escritorio remoto, pero el cual no será grabado como macro.

Los tres perfiles grabados son los siguientes:

- **Perfil ofimático**: sobre él grabamos distintas pulsaciones de teclado y ratón abriendo un archivo de bloc de notas, escribiendo sobre él, guardándolo, moviendo su ventana activa por la pantalla, maximizando y minimizando ventana, copiar archivo, pegarlo, etc.

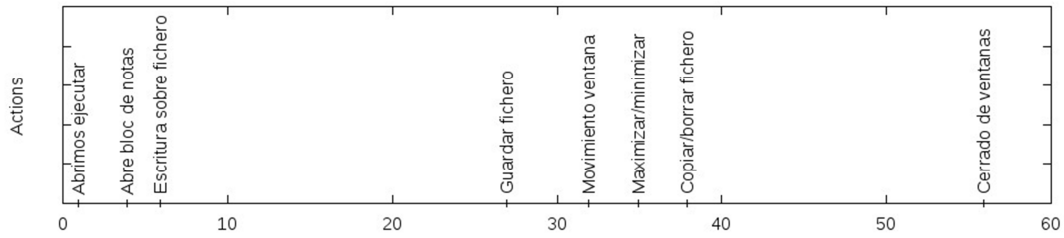

Figura 2.10. Acciones del perfil ofimático

- **Perfil de navegación**: en él grabamos un acceso a un navegador Web para acceder a una página Web con una necesidad de recursos muy alta, como es www.marca.com, navegar sobre ella un tiempo moderado

y, posteriormente, acceder a una página Web menos necesitada de recursos como es www.tlm.unavarra.es en la que también navegamos un poco sobre ella.

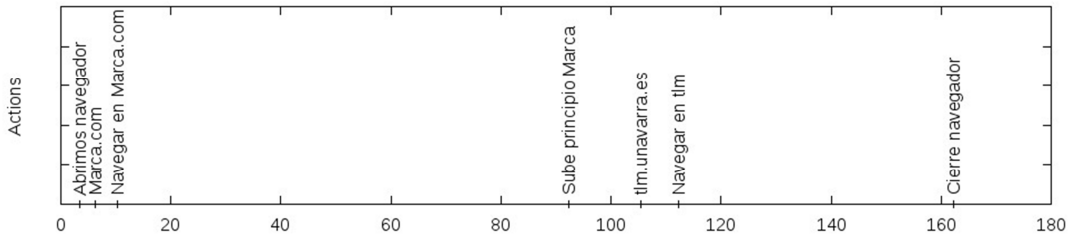

Figura 2.11. Acciones del perfil de navegación

- **Perfil audiovisual**: es el perfil que más ancho de banda de red nos consume, ya que accedemos a www.youtube.com y entramos a un vídeo donde un joven nos habla sobre Amazon WorkSpaces y en él podemos bastante variación de píxeles porque gesticula con los brazos y, por ello, nos aprovechamos de ello para ir modificando las diferentes calidades que nos ofrece el servicio de Youtube y ver cómo se puede observar un vídeo a través de un escritorio remoto.

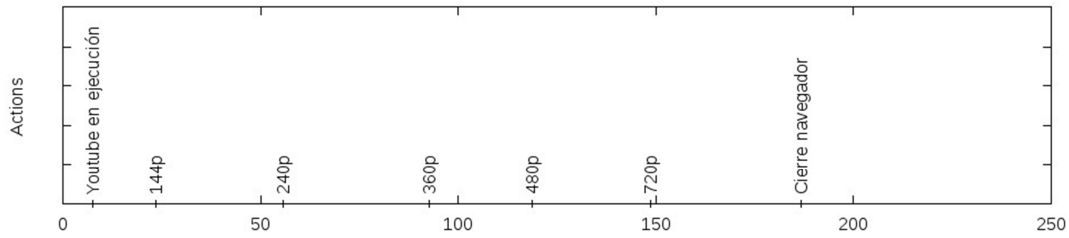

Figura 2.12. Acciones del perfil audiovisual

3. Efectos analizados

Una vez obtenidas las diferentes capturas de tráfico con Wireshark, podemos observar la comparación entre diferentes tipos de efectos que pueden surgir tanto en protocolos como RDP, VNC o TeamViewer. Por ello hemos obtenido de cada captura sus instantes de tiempo y sus velocidades en cada instante con un paquete que ofrecen las máquinas Linux llamado *tcpstat* [10]. Ese paquete lo que hace es sacarte un archivo de datos donde nos extrae los instantes de tiempo y velocidades nombradas anteriormente de cada tráfico de subida y bajada. Los comandos de terminal correspondientes los hemos metido en un script [Anexo 1], y la forma de ejecutarlo será:

sh tcpstat.sh PerfilOfiRDP PerfilOfiRDP_DL PerfilOfiRDP_UL

Donde el primer parámetro es el nombre de la captura de wireshark .pcap y los dos otros parámetros serán los nombres de las datas de salida con los datos obtenidos.

Una vez extraídos los datos, los plasmamos gráficamente con *gnuplot* [9], otra herramienta de Linux. En el gráfico lo etiquetamos con los diferentes movimientos que ha hecho la macro para saber, en cada instante de tiempo, cuántos recursos ha consumido cada acción.

Para crear las gráficas hemos creado un script [Anexo 2], donde directamente se introducen las capturas de tráfico (downstream y upstream), el fichero con las etiquetas preparadas y el nombre del archivo final como imagen que se desea para obtener finalmente el gráfico.

Por ejemplo: *sh plot.sh PerfilOfiRDP_DL PerfilOfiRDP_UP PerfilOfi PerfilOfimatico_RDP*

Los archivos PerfilOfiRDP_DL y PerfilOfiRDP_UP tienen la siguiente forma:

```
0.724531889 1992
1.724531889 57928
2.724531889 90696
3.724531889 8776
4.724531889 7984
5.724531889 80240
6.724531889 2064
7.724531889 8352
8.724531889 11456
9.724531889 10944
```

Figura 3.1. Formato de los archivos de información.

donde la primera columna se refiere al eje del tiempo y la segunda columna se refiere a Downstream/Upstream (bps) en cada instante de tiempo.

Y el archivo PerfilOfi, que es el de etiquetado, tiene la siguiente forma:

```
2.724531889 0 "Accedemos al Ejecutar"
5.724531889 0 "Notepad en ejecución"
8.724531889 0 "Escritura sobre el fichero"
40.724531889 0 "Guardar fichero"
44.724531889 0 "Movimiento de ventana"
52.724531889 0 "Maximizado de ventana"
56.724531889 0 "Minimizado de ventana"
64.724531889 0 "Apertura explorador de Windows"
72.724531889 0 "Copiado/borrado de fichero"
74.724531889 0 "Cerrar ventana"
```

Figura 3.2. Formato de los archivos de etiquetado

donde la primera columna se refiere al tiempo (eje X) y la tercera columna son las etiquetas en cada instante de tiempo (eje Y).

El propósito es ver cómo trabajan los distintos servicios para luego analizarlos más profundamente en varias limitaciones de red.

El primer análisis constará de ver qué ancho de banda consume cada acción en cada servicio sin ninguna limitación sobre la red utilizando como cliente un sistema operativo Windows. Posteriormente, se procederá a un análisis añadiendo limitaciones.

3.1. Análisis sin conformación de tráfico sobre Windows

3.1.1. Problemas encontrados en VNC

Este protocolo, en la visualización de vídeos, va muy justo de calidad, con muchas saturaciones y muchas paradas. Por lo que hemos querido intentar mejorar esa visualización ya que Amazon parece que limita el protocolo VNC a una velocidad de entre 6-8 Mbps:

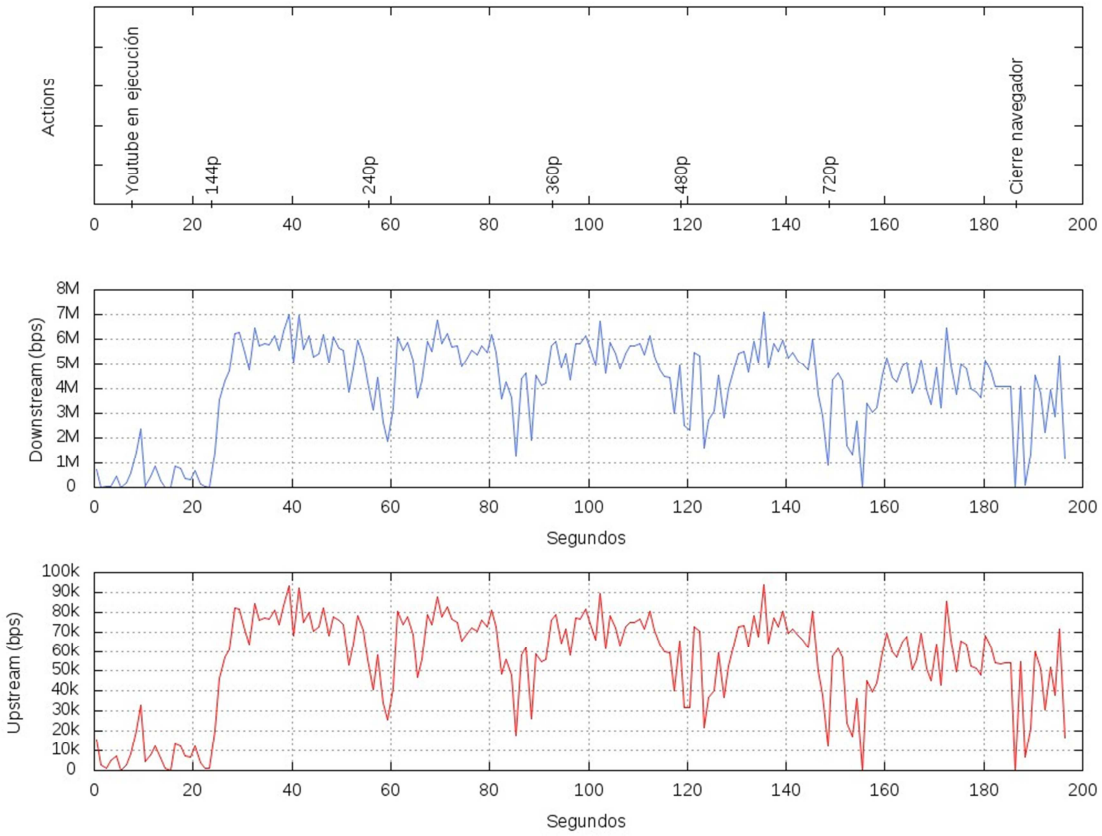

Figura 3.3. Perfil audiovisual sobre protocolo VNC

Entonces hemos realizado varias pruebas para ver cuál era el posible problema:

- Crear una VPN con n2n entre el cliente y el servidor

Hemos creado una red privada virtual para ver si era algún problema de la red. Para ello hemos configurado una red P2P con n2n [11] y hemos instalado tanto

en el servidor un supernodo y su respectivo nodo, y en el cliente un nodo. Para el servidor Windows lo hemos descargado de http://luca.ntop.org/n2nWin32/binary/ y para el cliente Linux de https://sourceforge.net/projects/ntop/files/n2n/. Una vez instalados ambos paquetes, para configurar el supernodo en el servidor hemos escrito en "cmd", en modo administrador, lo siguiente:

cd Desktop\n2n-Win32\bin\supernode.exe -l 5000

Así escucha nuevas conexiones a la VPN por el Puerto 5000

Y como nodo hemos puesto lo siguiente:

cd Desktop\n2n-Win32\bin\edge.exe -l 52.58.116.38:5000 -c prueba -k 78752626m -a 10.0.0.10

donde –l establece el supernodo al que queremos conectarnos, -c el nombre de comunidad a la que nos queremos unir, -k la contraseña que establecemos a la red y –a la IP que obtendrá el equipo en la VPN.

Como en el servidor, el cliente también se le establece una configuración para unirse a la red. Para ello, abrimos terminal y escribimos lo siguiente:

cd Escritorio/n2n/n2n-1.3.2/

Todas las rutas expuestas dependerán de donde se haya instalado los archivos.

Una vez dentro de la carpeta n2n-1.3.2, pondremos lo siguiente:

sudo edge -d edge0 -l 52.58.116.38:5000 -c prueba -k 78752626m -a 10.0.0.20

donde –d es el interfaz virtual que se crea y el resto de parámetros, los mismos que en el sistema operativo Windows.

Finalmente, abrimos el puerto 5000 desde "Security Groups" de Amazon EC2:

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	5000	0.0.0.0/0
All ICMP	All	N/A	0.0.0.0/0
Custom UDP Rule	UDP	5000	0.0.0.0/0

Figura 3.4. Puertos para VPN

Una vez abiertos, podremos comprobar haciendo ping entre ambos equipos que existe conexión a través de la VPN.

Una vez creada la VPN, comprobamos si el protocolo VNC sufría limitaciones de red, y sí, seguía sufriendo limitaciones así que procedimos a crear un servidor FTP para ver si sufría limitaciones, como le está ocurriendo al servidor VNC.

- Habilitar un servidor FTP

Para ello hemos instalado Filezilla Server [12], un servidor FTP muy utilizado. Lo hemos descargado de la página principal https://filezilla-project.org/ y lo hemos instalado. Durante la instalación, hemos añadido un usuario de prueba que le permita tanto descargarse como subir ficheros al servidor.

Una vez terminada la configuración del servidor FTP, se ha procedido a abrir los puertos correspondientes para FTP:

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	11000 - 12000	0.0.0.0/0
Custom TCP Rule	TCP	21	0.0.0.0/0
Custom TCP Rule	TCP	20	0.0.0.0/0

Figura 3.5. Puertos para el servidor FTP

Una vez abiertos los puertos, ya puede conectarse un cliente Filezilla al servidor y probar descargando un archivo si Amazon sigue limitándo:

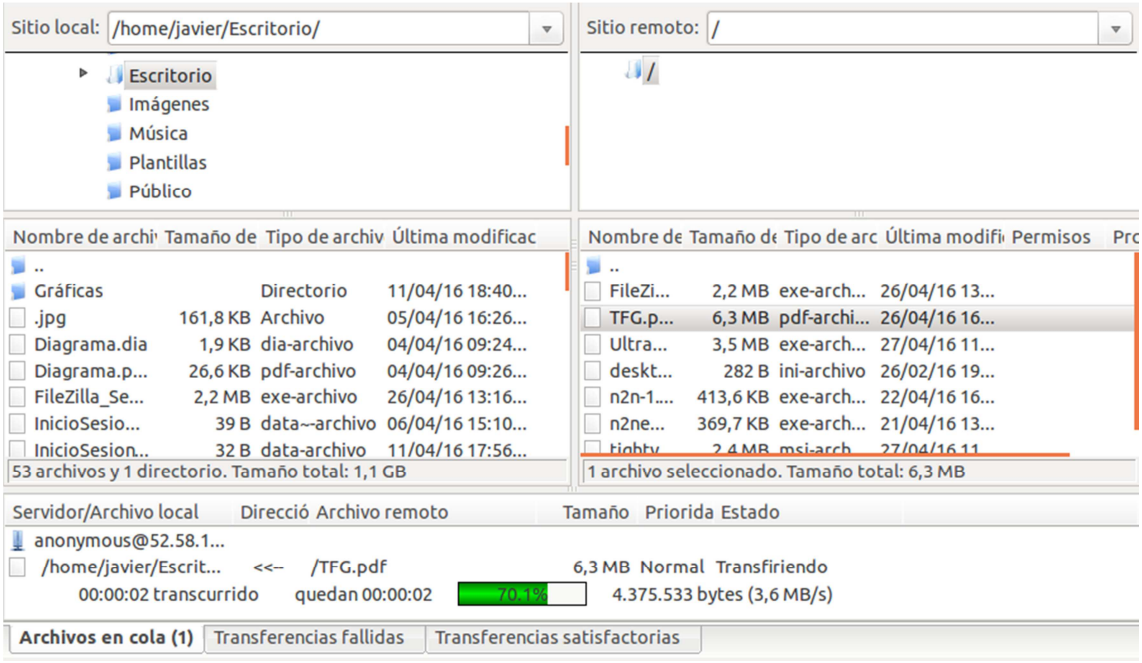

Figura 3.6. Cliente Filezilla descargando fichero

Como podemos observar, el fichero ser esta descargando a unos 3.6 MB/s que equivale a unos 30Mbps, por tanto, Amazon no nos limita el servidor FTP.

También hemos probado a cambiar la versión del servidor VNC, instalando UltraVNC de su página oficial http://www.uvnc.com/ y seguía existiendo ese

problema. Además, también se probó a cambiar la codificación de imagen en las opciones avanzadas que ofrece VNC, pero sin mejora alguna, ya que la codificación por defecto que tiene, ZRLE, es la que mejor nos visualiza.

Lo siguiente que hemos intentado ha sido crear un túnel SSH entre el servidor y el cliente para ver si así nos limita el servidor VNC.

- Tunel SSH

Para intentar minimizar o resolver el problema de la limitación de red existente con el protocolo VNC, hemos creado un túnel SSH que vaya desde nuestro servidor hasta la máquina cliente. [13].

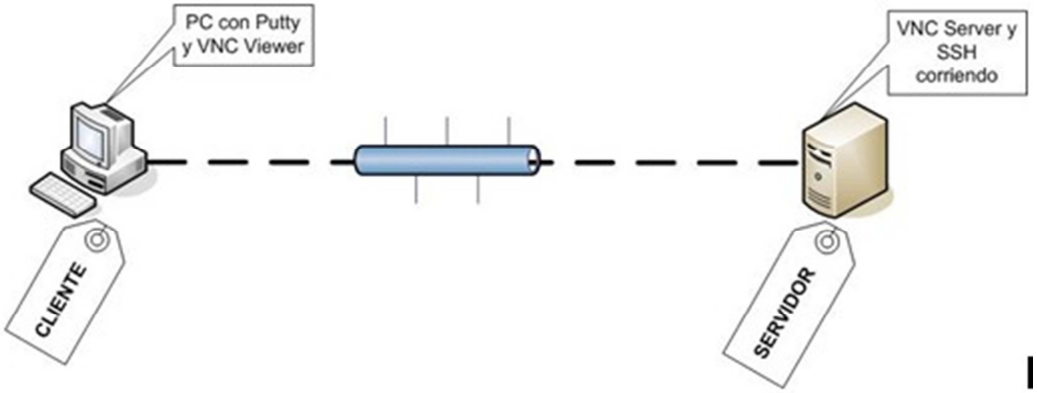

Figura 3.7. Tunel SSH

Primero, hemos instalado y configurado un servidor SSH, descargado de su web oficial http://www.freesshd.com/, sobre nuestro servidor, con una encriptación baja (AES 128 bits), pudiendo acceder a él a través de una cuenta creada y sobre el puerto TCP 22.

Una vez tenemos en funcionamiento nuestro servidor SSH, desde el cliente podemos configurar el túnel, instalando un cliente SSH llamado "*PuTTY*", el cuál se puede descargar de su página oficial http://www.putty.org/. Dentro del panel "*Category*" de PuTTY, configuraremos sobre la pestaña "*Session*" la IP de nuestro servidor donde nos queremos conectar y el puerto por el cual nos queremos conectar, por ejemplo:

Host: 52.58.163.232 Port: 22

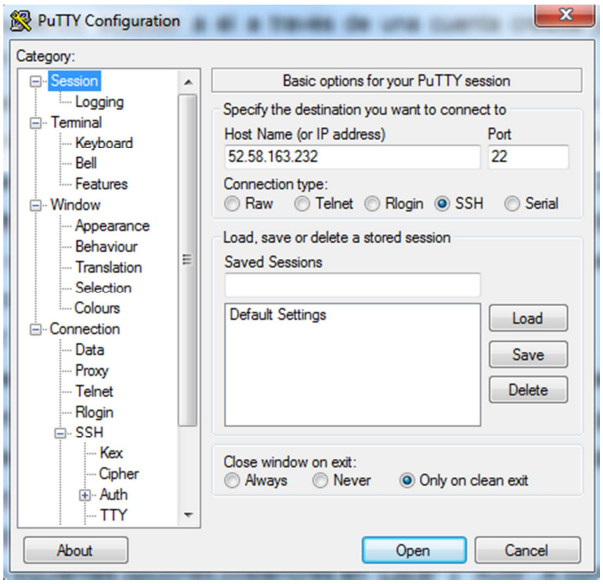

Figura 3.8. Configuración PuTTY (1)

Posteriormente, sobre la pestaña Connection/SSH/Tunnels, añadimos un nuevo puerto, donde en nuestro caso queremos que sea el puerto por el cual nos conectamos al servidor VNC, es decir, el puerto 5900. Por ejemplo:

Source port: 5900

Destination: 52.58.163.232:5900

dejando las siguientes opciones posteriores en "*Local*" y "*Auto*". A continuación, se pulsa sobre el botón "Add" y ya tenemos preparado el túnel, solo faltaría abrir la conexión mediante el botón "Open", después iniciando sesión sobre SSH mediante la cuenta creada anteriormente en la configuración del servidor SSH.

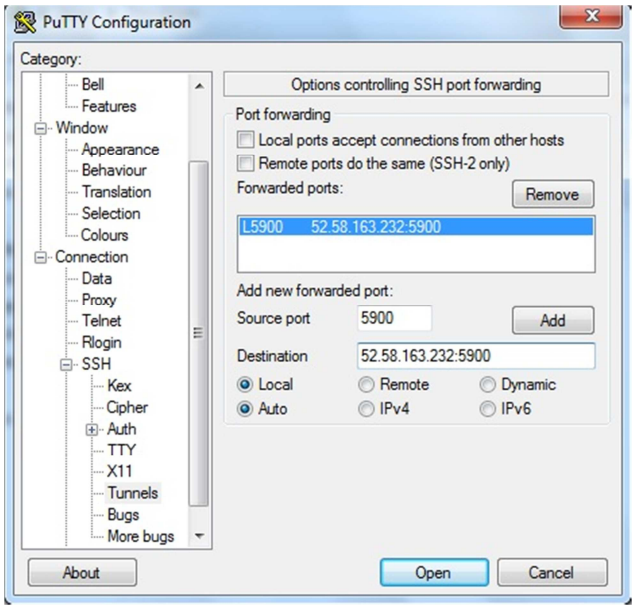

Figura 3.9. Configuración PuTTY (2)

Una vez iniciada la sesión SSH, ya podemos conectarnos a través de VNC. Por tanto, ejecutamos VNC Viewer y como host del servidor pondremos: localhost:5900 y así accederemos al servidor a través del túnel SSH creado.

Como el problema lo teníamos principalmente sobre el perfil audiovisual, hemos realizado una nueva captura sobre ese perfil y los resultados han mejorado en cuanto a su tasa de bit, como se puede ver en el apartado 3.1.3, referente al protocolo VNC, pero respecto a su calidad de imagen sigue siendo bastante limitada.

Además, sobre el túnel SSH también hemos comprobado si el servidor SFTP estuviese limitado y este ha sido el resultado:

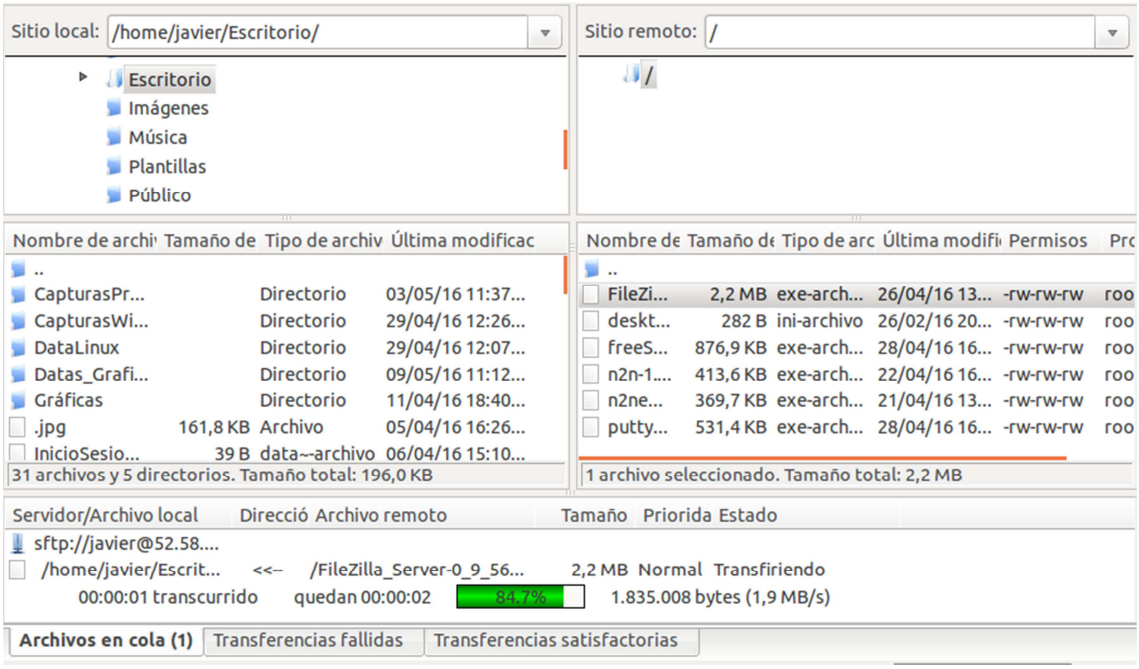

Figura 3.10. Servidor SFTP sobre túnel SSH

Donde observamos una tasa de bajada de 1.9 MB/s que, equivale aproximadamente unos 16 Mbps, por tanto, no sufre limitación.

3.1.2. Protocolo RDP

Para este protocolo, hemos obtenido los siguientes resultados:

- Inicio de sesión sobre el servicio

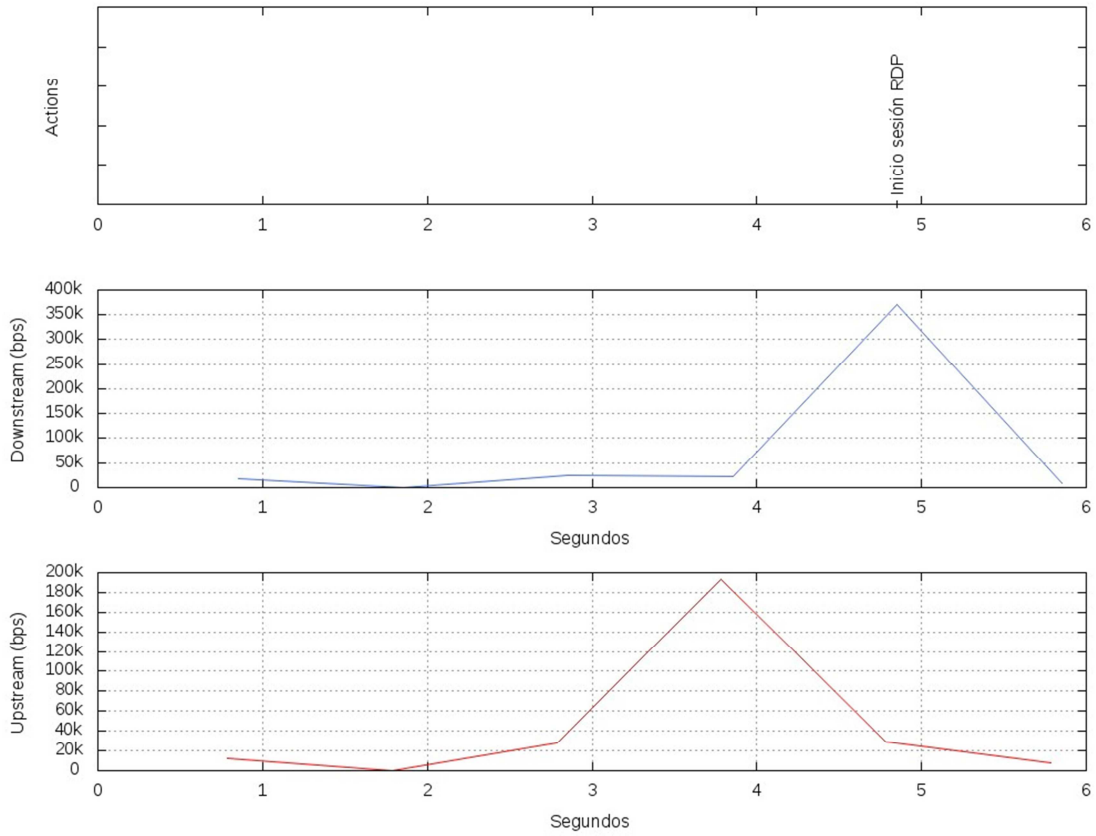

Figura 3.11. Inicio de sesión sobre protocolo RDP

Sobre la imagen podemos observar como el inicio de sesión con el protocolo utilizado en los escritorios remotos de Windows, consume unos 400Kbps de ancho de banda de bajada y unos 200Kbps de subida.

- Perfil ofimático

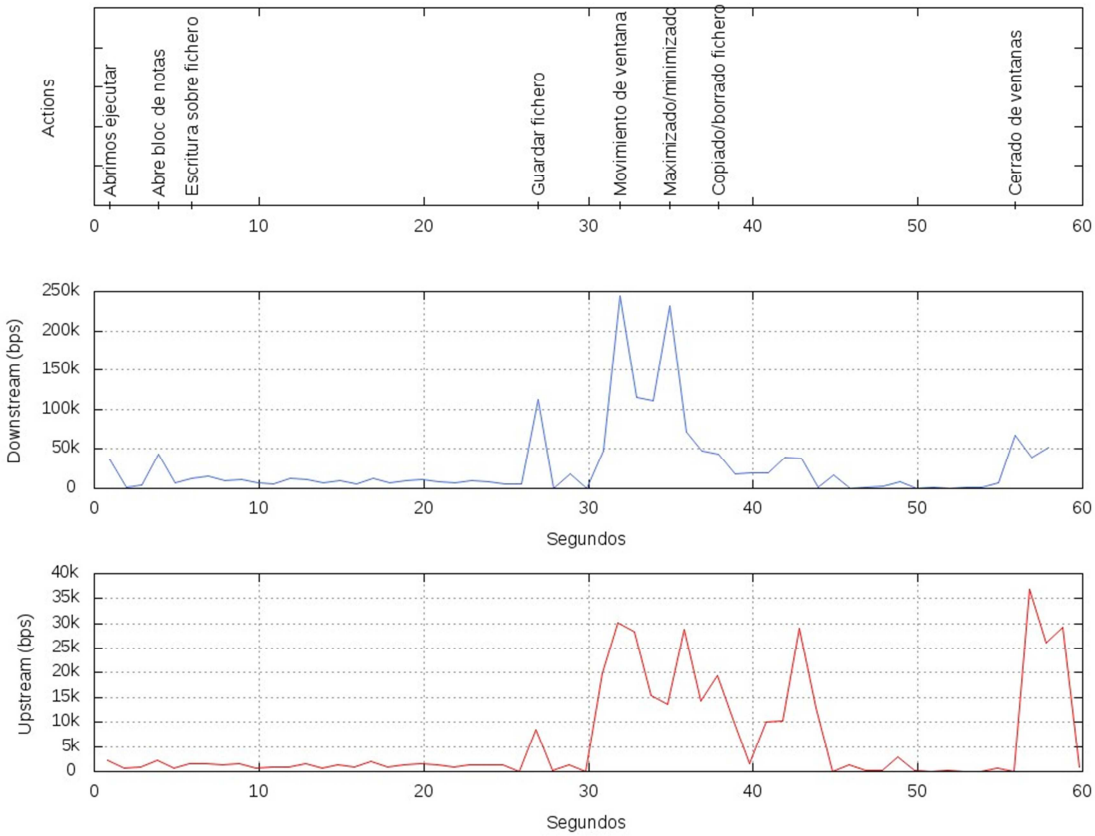

Figura 3.12. Perfil ofimático sobre protocolo RDP

Sobre él podemos observar, como los movimientos de ventana o las aperturas de nuevas ventanas son las acciones que más ancho de banda requieren en este perfil, pudiendo llegar a los 250Kbps de bajada y los 40Kbps de subida.

- Perfil de navegación

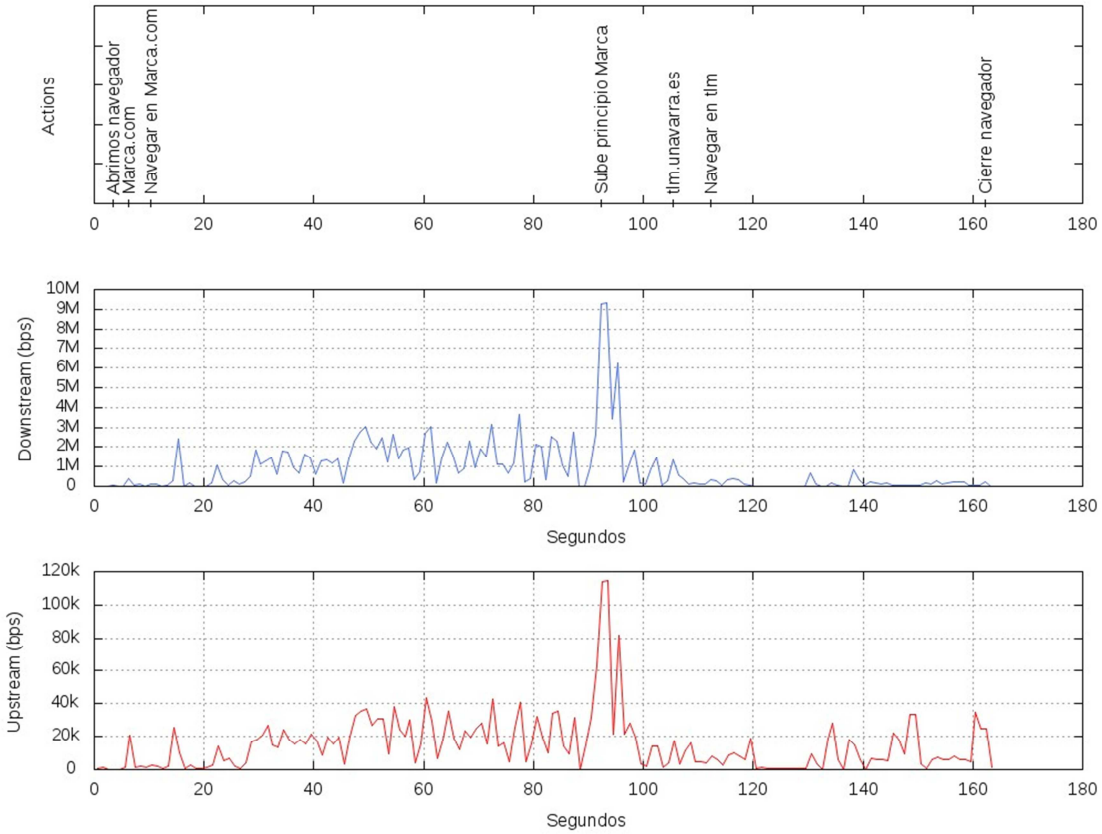

Figura 3.13. Perfil de navegación sobre protocolo RDP

Sobre este perfil observamos la gran diferencia que existe en navegar en diferentes páginas Web según el contenido de cada una de ellas. Por ello, navegar en www.marca.com, una web con mucho contenido publicitario con animaciones, consume bastante más que una web con poco contenido publicitario, como www.tlm.unavarra.es. En Marca, se llega a velocidades de 9Mbps de bajada y 120Kbps de subida, y en tlm a velocidades muy bajas, entorno a 1Mbps de bajada y 40Kbps de subida.

- Perfil audiovisual

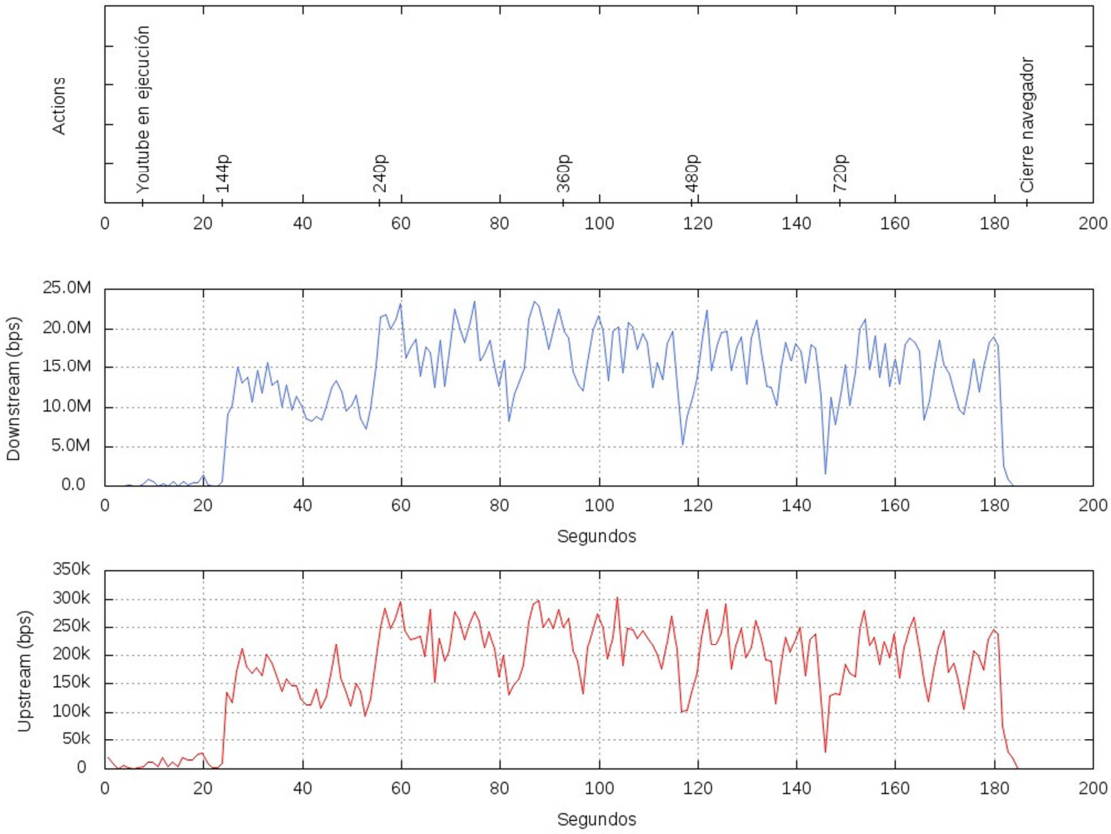

Figura 3.14. Perfil audiovisual sobre protocolo RDP

Este perfil llega a unos anchos de banda mayores que el resto por su alto contenido audiovisual, hasta el punto de llegar a velocidades entorno a 25Mbps de bajada y 350Kbps de subida.

3.1.3. Protocolo VNC

Para este protocolo, hemos obtenido los siguientes resultados:

- Inicio de sesión sobre el servicio

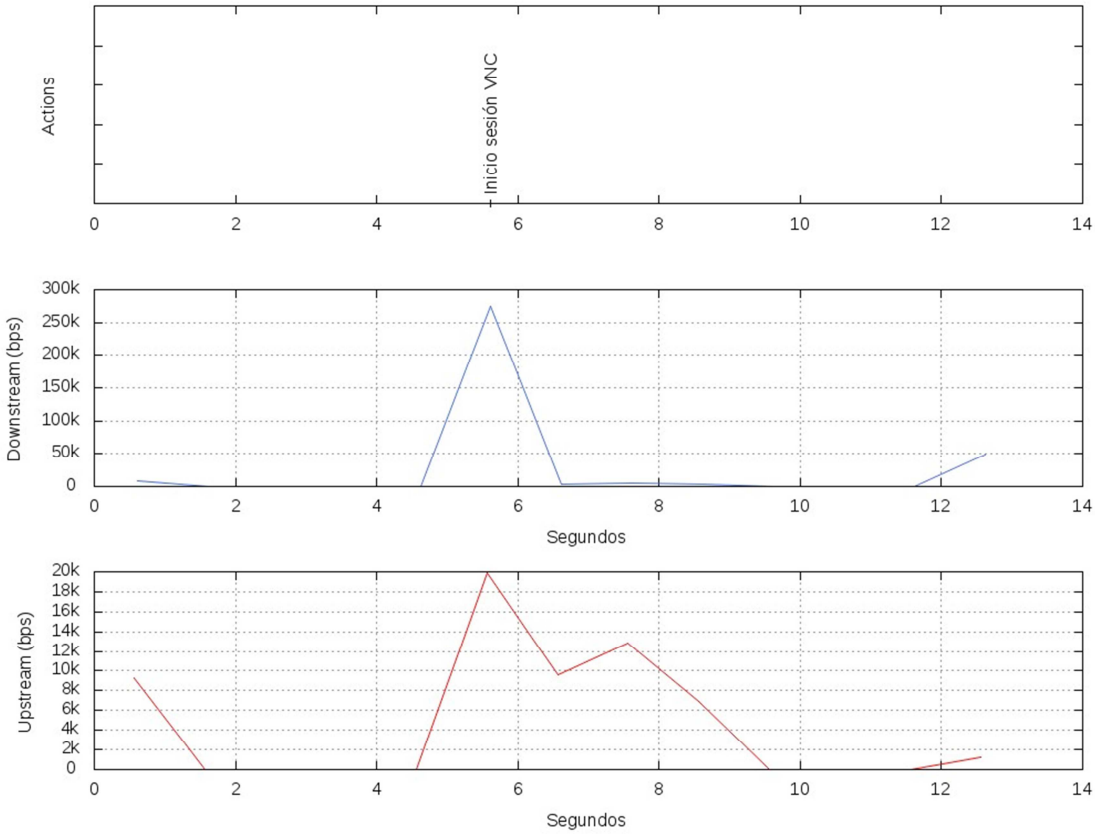

Figura 3.15. Inicio de sesión sobre protocolo VNC

Sobre este protocolo observamos cuánto ancho de banda consume de bajada (300Kbps) y cuánto de subida (20Kbps) iniciando sesión sobre el protocolo VNC.

- Perfil ofimático

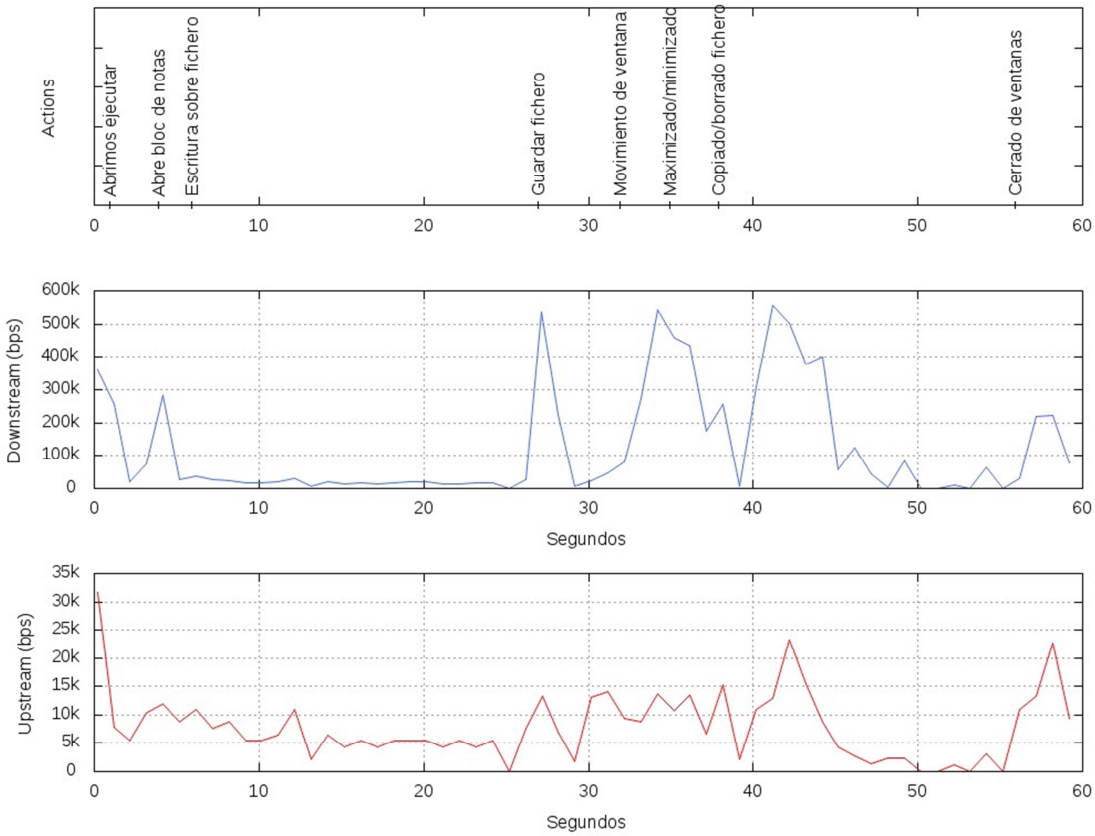

Figura 3.16. Perfil ofimático sobre protocolo VNC

Observamos, como ocurría en el protocolo RDP, como las acciones de movimiento de ventana, aperturas de ventana, etc. son las acciones que más ancho de banda consumen en este perfil, llegando a 600Kbps de bajada y 25Kbps de subida.

- Perfil de navegación

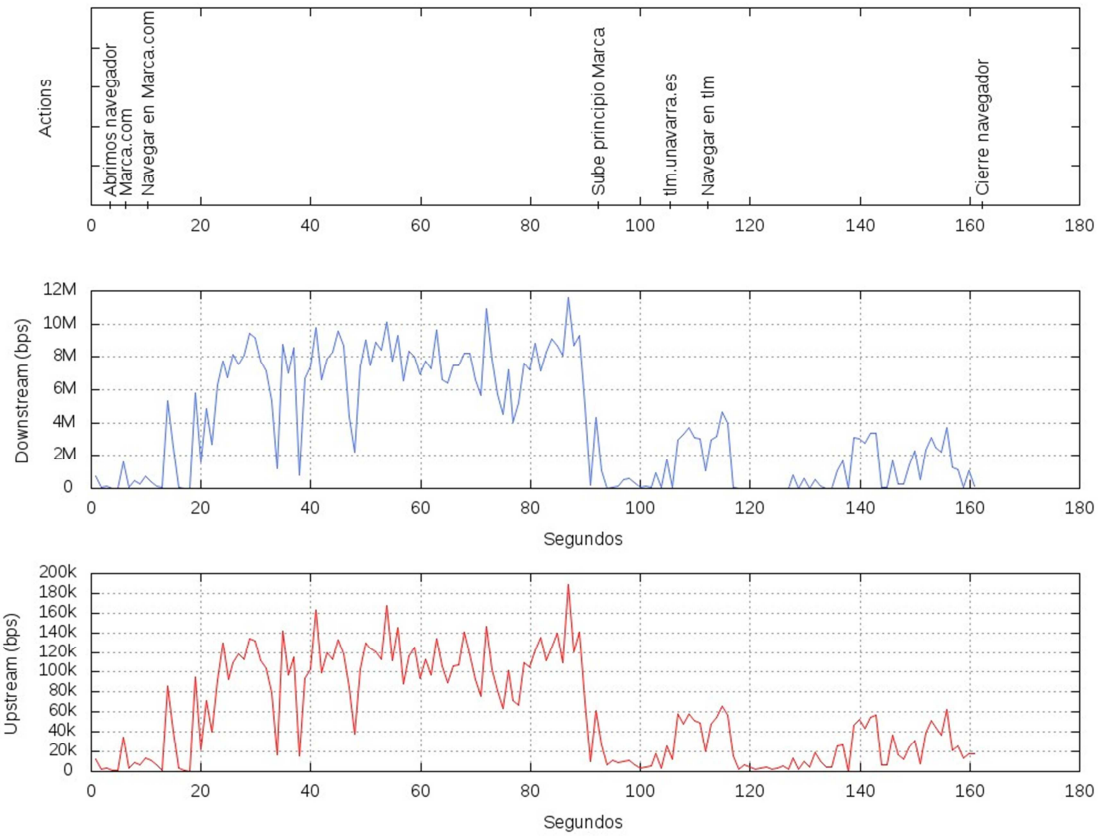

Figura 3.17. Perfil de navegación sobre protocolo VNC

Como se puede ver y como ocurría sobre RDP, la página de www.marca.com consume a mucha mayor escala que www.tlm.unavarra.es hasta tal punto de llegar a velocidades de casi 12Mbps de bajada y 200Kbps de subida. Recalcar que sobre este protocolo el navegador va mucho más lento en desplazamiento del scroll, en el cargado de imágenes y, en muchos casos, muy saturado por el propio protocolo.

- Perfil audiovisual

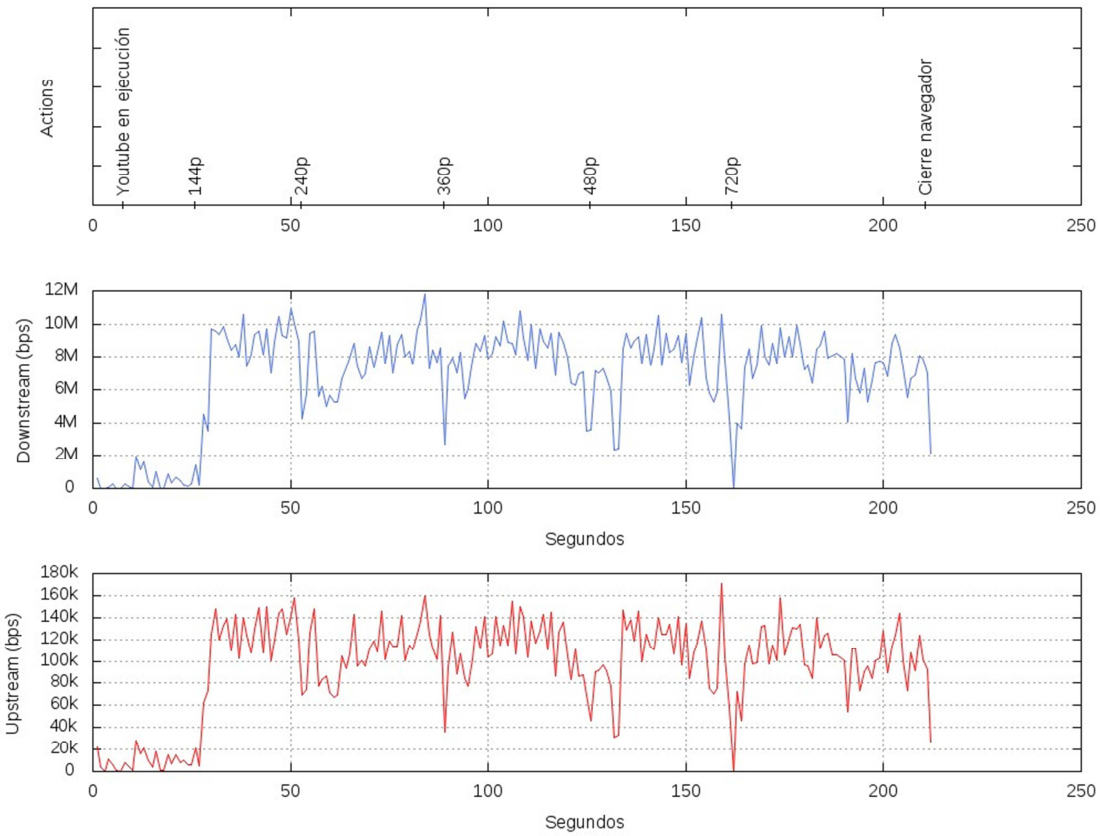

Figura 3.18. Perfil audiovisual sobre protocolo VNC a través de un túnel SSH

Podemos observar como el perfil ha aumentado ligeramente su ancho de banda hasta los 12 Mbps de bajada y los 180 Kbps de subida. Por tanto, hemos podido minimizar un poco el problema existente con la limitación del protocolo que existe en los servidores Amazon.

3.1.4. TeamViewer

- Inicio de sesión sobre TeamViewer

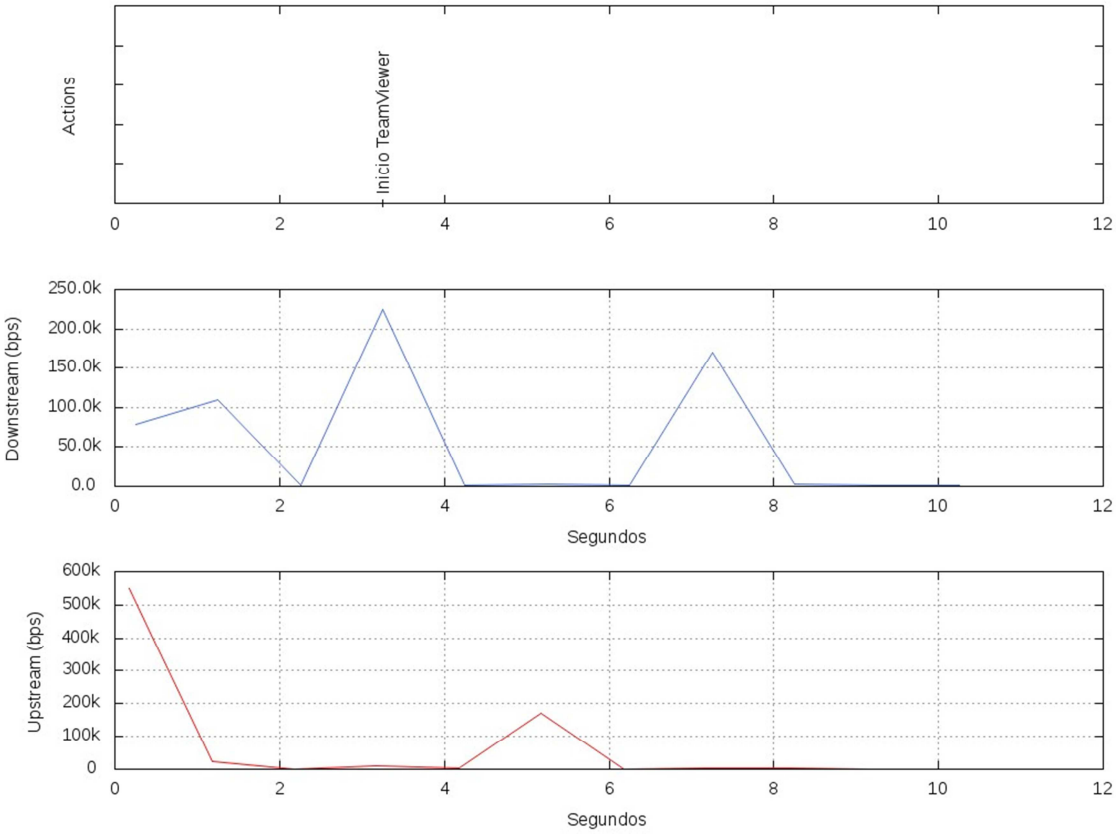

Figura 3.19. Inicio de sesión con TeamViewer

Observamos como iniciar sesión sobre TeamViewer consume una tasa de 250Kbps de bajada aproximadamente, y una tasa de subida de pocos Kbps (10 Kbps aproximadamente).

- Perfil ofimático

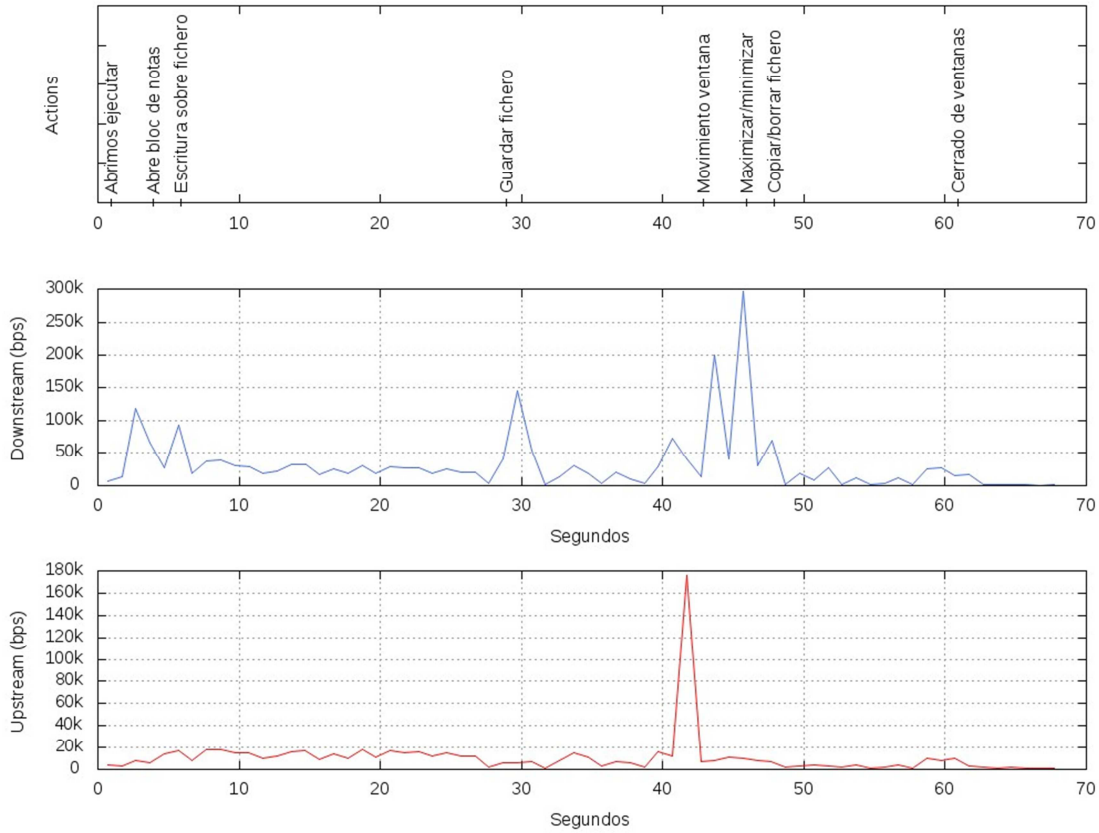

Figura 3.20. Perfil ofimático sobre TeamViewer

Observamos, como ocurría en el resto de protocolos, como el movimiento de ventana o el maximizado o minimizado de ella son los instantes de tiempo donde más se consume tráfico sobre este perfil, llegando a los 300 Kbps de bajada y 180 Kbps de subida.

- Perfil de navegación

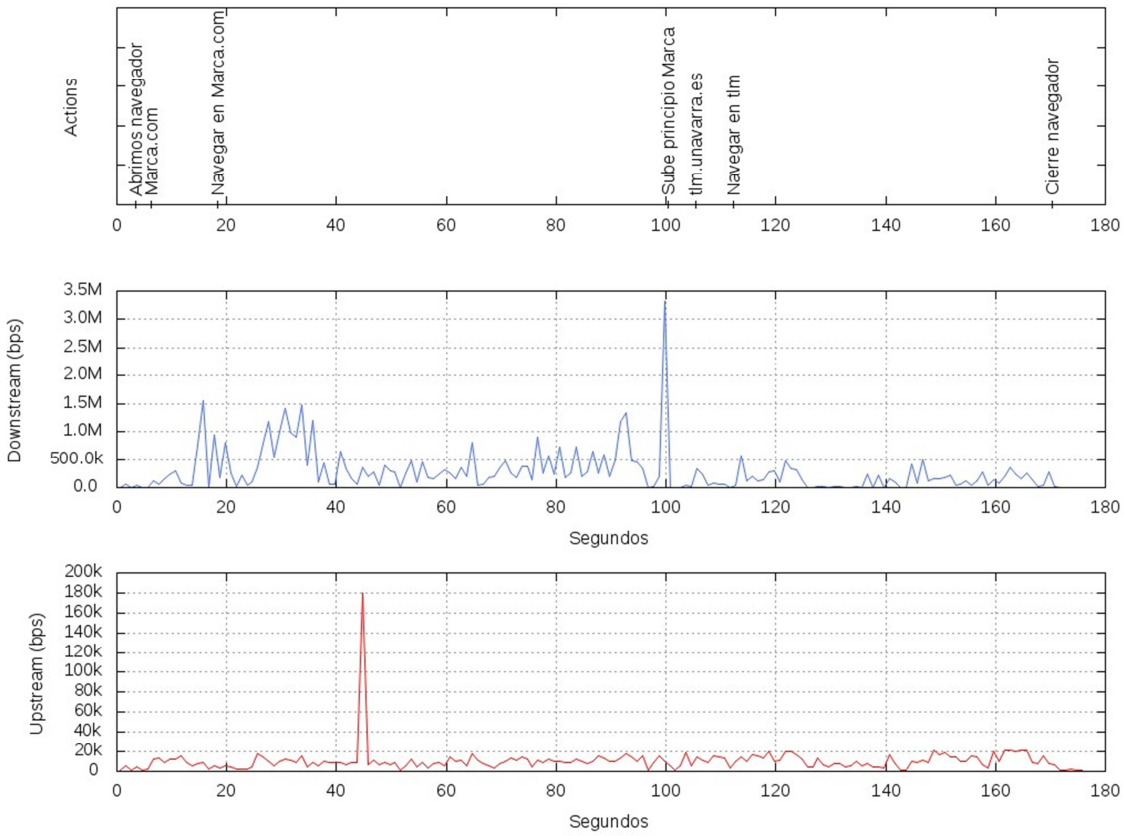

Figura 3.21. Perfil de navegación sobre TeamViewer

Sobre este perfil, observamos como consume más navegar por una página con alto contenido publicitario (Marca) respecto a una sin contenido publicitario (tlm.unavarra.es). Como ocurre en el resto de protocolos, en el momento de subir al principio del periódico Marca, hay un pico de tasa que, en este caso, llega a los 3.5 Mbps de bajada. El máximo de subida ocurre un poco antes, navegando sobre el periódico, a una tasa pico de 180 Kbps.

- Perfil audiovisual

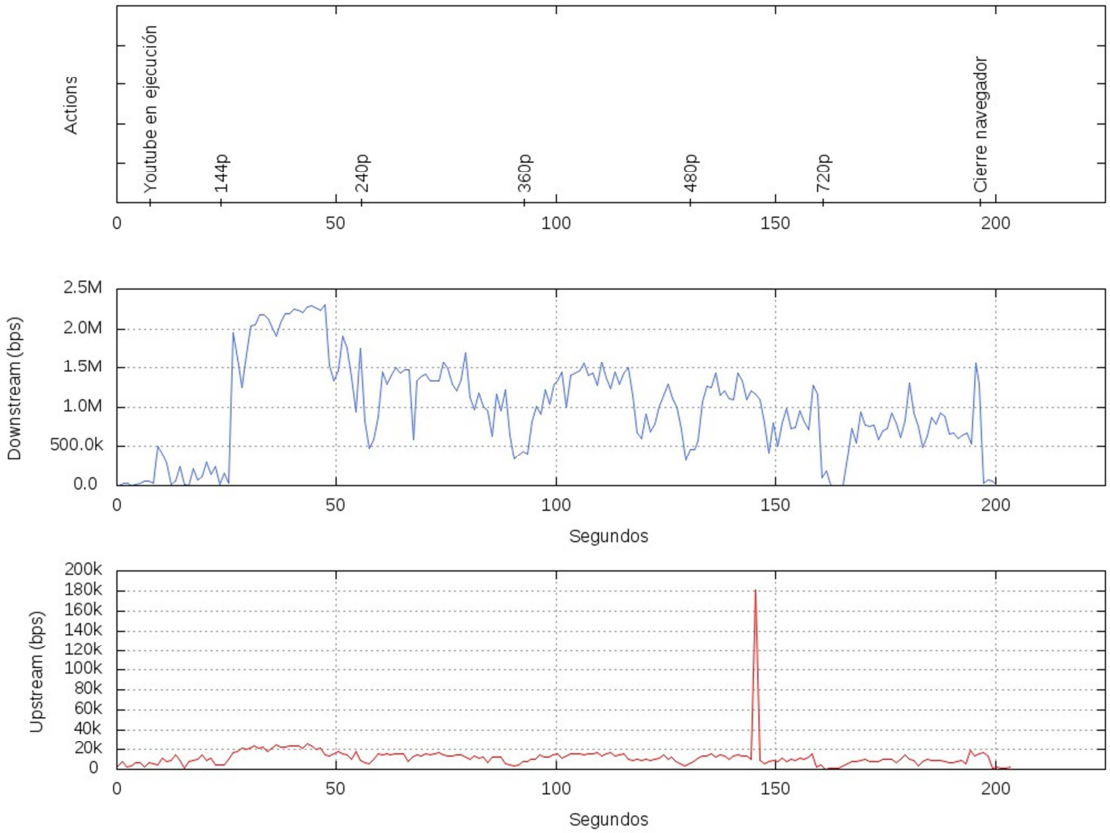

Figura 3.22. Perfil audiovisual sobre TeamViewer

Observamos, sobre este perfil, como la tasa media de bajada es una tasa muy pequeña para ser un perfil de estas características, pero también se puede asegurar, que la calidad de vídeo no es mala (similar a RDP). Tampoco se puede comprobar la tasa que habrá a través de un túnel SSH debido a que existe un servidor, propiedad de TeamViewer, de por medio. Por tanto, establecemos una tasa de bajada máxima de unos 2.5 Mbps y una tasa de subida de unos 180 Kbps.

3.1.5. Tablas comparativas

A continuación, se muestra una tabla comparativa de los protocolos con cada uno de sus perfiles analizados, exponiendo su tasa media, tasa de pico y tasa total transferida en ambos sentidos, calculada sobre Excel mediante las funciones PROMEDIO, MÁX y SUMA, respectivamente.

Perfil	**Inicio de sesión**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	74 Kbps	45 Kbps	27 Kbps	4,7 Kbps	54 Kbps	19,7 Kbps
Tasa pico	371 Kbps	193 Kbps	274 Kbps	20 Kbps	224 Kbps	170 Kbps
Total (Bytes)	55,5 KB	34 KB	43 KB	7,5 KB	74 KB	27 KB
Calidad	5		5		5	
Perfil	**Ofimático**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	29 Kbps	6 Kbps	126 Kbps	8 Kbps	32 Kbps	11 Kbps
Tasa pico	245 Kbps	37 Kbps	556 Kbps	32 Kbps	296 Kbps	175 Kbps
Total (Bytes)	209 KB	48 KB	945 KB	59 KB	272 KB	92 KB
Calidad	5		5		5	

Perfil	Navegación					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	900 Kbps	15 Kbps	3,9 Mbps	60 Kbps	281 Kbps	10,6 Kbps
Tasa pico	9,4 Mbps	115 Kbps	11,6 Mbps	189 Kbps	3,3 Mbps	180 Kbps
Tasa total	18 MB	309 KB	78 MB	1,2 MB	6,2 MB	233 KB
Calidad	5		4		4	
Perfil	Audiovisual					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	13 Mbps	172 Kbps	6,8 Mbps	96 Kbps	962 Kbps	12 Kbps
Tasa pico	23,4 Mbps	303 Kbps	11,8 Mbps	171 Kbps	2,3 Mbps	181 Kbps
Tasa total	300 MB	4 MB	181 MB	2,6 MB	25 MB	310 KB
Calidad	5		1		4	

Tabla 1: Resultados sin limitación

Calidad: Se medirá subjetivamente a escala 1-5, de la siguiente manera:

- ***1: Muy mala***.

  Inicio de sesión: Tarda muchísimo en acceder al escritorio remoto, incluso a veces da errores de cierre por tiempo de espera excedido.

  Ofimático: Se salta procesos de acciones, movimiento de ventana a saltos agigantados, escritura sobre el fichero muy lenta.

  Navegación: Es imposible leer los artículos, no carga las imágenes, el scroll vertical va muy lento.

Audiovisual: Vídeo a saltos, muy píxelado en todas las calidades de imagen, sin continuidad en la imagen.

- ***2: Mala***.

  Inicio de sesión: Tarda mucho en acceder al escritorio remoto

  Ofimático: Movimiento de ventana lento, escritura sobre el fichero lenta. Apertura de ventanas lenta.

  Navegación: Saltos de scroll que impiden leer algunas noticias, solo carga algunas imágenes o la mitad de ellas.
  Audiovisual: Vídeo a saltos, muy píxelado en las calidades de imagen altas, sin continuidad en la imagen.

- ***3: Regular***.

  Inicio de sesión: Le cuesta un rato acceder al escritorio remoto, pero sin llegar a suceder errores.
  Ofimático: Acciones con pequeño retardo (movimiento de ventana, escritura).
  Navegación: Movimientos de scroll lentos, imágenes de gran tamaño tardan en cargarse, anuncios publicitarios en movimiento van con retardo.
  Audiovisual: Imágenes pixeladas en todas las calidades, calidades altas (HD, 480p) menos continuidad de movimiento que las calidades más bajas (144p, 240p).

- ***4: Buena***.

  Inicio de sesión: Tarda un poco en acceder pero sin ningún problema añadido.
  Ofimático: Escritura sobre el fichero con normalidad, movimientos de ventana estables con algún pequeño retardo.
  Navegación: Movimientos de scroll estables, anuncios publicitarios en movimiento van con retardo, las noticias son leídas perfectamente.

Audiovisual: Imágenes en movimiento en la mayor parte de las calidades de vídeo. Puede haber problemas de continuidad de imagen en calidades como 720p o 1080p.

- ***5: Muy buena***.

  Inicio de sesión: Accede al escritorio remoto al instante sin ningún tipo de problema.

  Ofimático: Escritura sobre el fichero con normalidad, movimientos de ventana estables, apertura de ventanas en el mismo instante.

  Navegación: Movimientos de scroll estables, anuncios publicitarios en movimiento se visualizan con claridad, las noticias son leídas perfectamente y todas las imágenes se cargan perfectamente.

  Audiovisual: Se puede visualizar un video en perfectas condiciones en todas las calidades disponibles sin ningún tipo de píxelado o parada sobre el vídeo.

3.2. Análisis con conformación de tráfico sobre Windows

Sobre este apartado analizaremos los resultados obtenidos para diferentes limitaciones configuradas sobre la red. Las limitaciones que hemos configurado son a 5Mbps, 2Mbps, 1Mbps y 300Kbps. Además la red tendrá un retardo añadido de 50 ms con un RTT total de 90 ms. La limitación a 300 Kbps la hemos configurado para situaciones en las que nos conectamos a un escritorio remoto con dispositivos móviles o tablets, los cuáles utilizan bajo ancho de banda.

Expondremos principalmente las gráficas de los perfiles que estén limitándose sobre la red. Para el caso de 300Kbps expondremos todos los perfiles, ya que es un ancho de banda bajo y el perfil ofimático puede llegar a saturarse en algunos instantes. Sobre las tablas comparativas quedarán reflejados todos los datos respecto a todos los perfiles.

3.2.1. Limitación a 5 Mbps

3.2.1.1. RDP

Sobre este protocolo no hemos encontrado limitación sobre el perfil ofimático ni el de navegación. Sus valores obtenidos aparecerán en la tabla comparativa posterior.

- Perfil de audiovisual

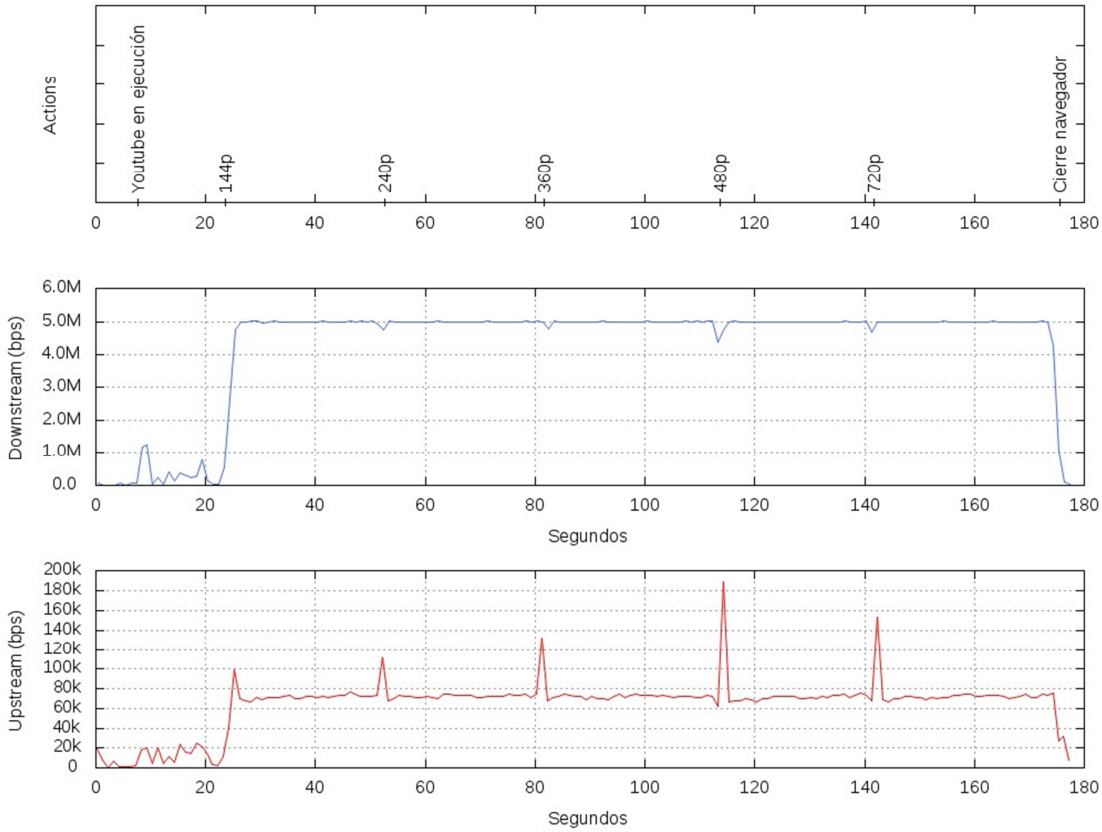

Figura 3.23. Perfil de audiovisual sobre protocolo RDP limitado a 5 Mbps

Podemos observar como el protocolo se limita a la velocidad de los 5 Mbps.

Relativo a la calidad, con calidad de video bajo (144p, 240p) se puede observar sin muchas dificultades. Conforme aumentamos esa calidad, empiezan a aparecer cortes de vídeo o imágenes píxeladas.

3.2.1.2. VNC

Sobre esta limitación, este protocolo se ve limitado en red en los perfiles de navegación y audiovisual. El perfil ofimático no se ve limitado. Sus datos aparecerán en la tabla comparativa posterior.

- Perfil de navegación

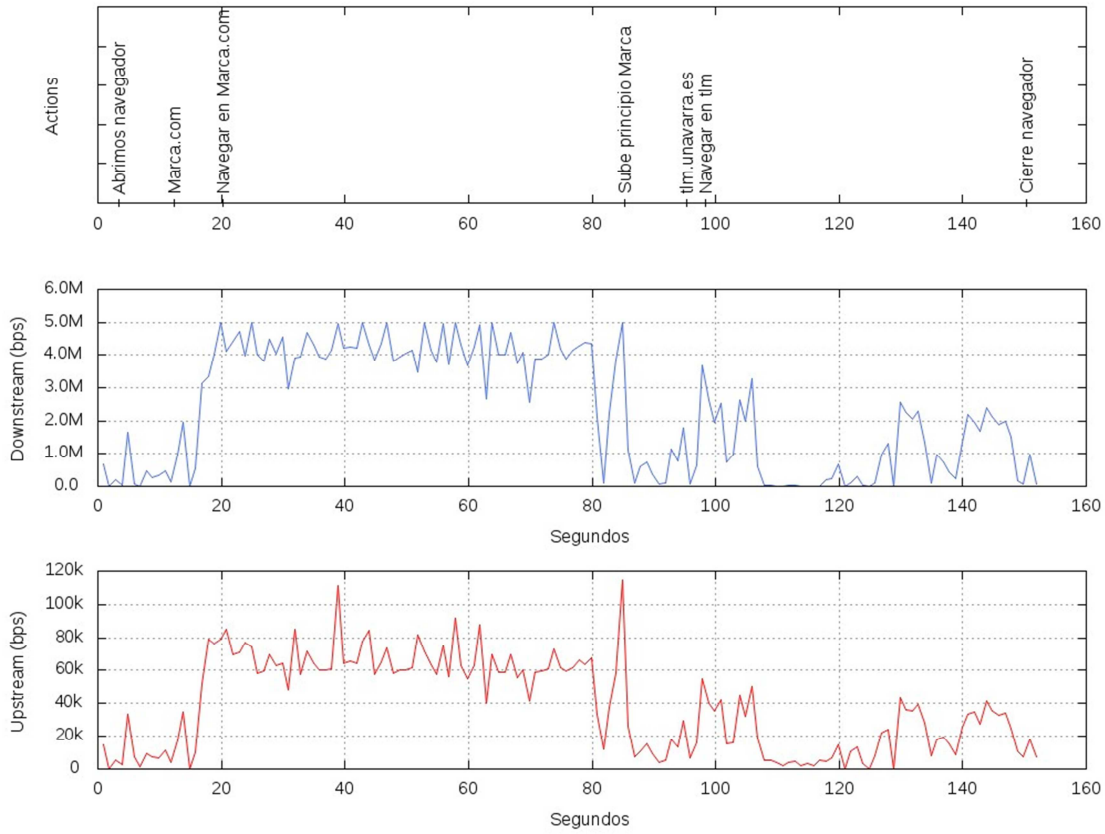

Figura 3.24. Perfil de navegación sobre protocolo VNC limitado a 5 Mbps

Podemos observar como este perfil es limitado cuando accede a Marca, una página con un alto contenido publicitario audiovisual, mientras que en la página de telemática no llega a sufrir esa limitación.

Sobre marca, las imágenes les cuesta cargar un poco más de lo habitual y el scroll vertical va con cierto retardo.

- Perfil audiovisual

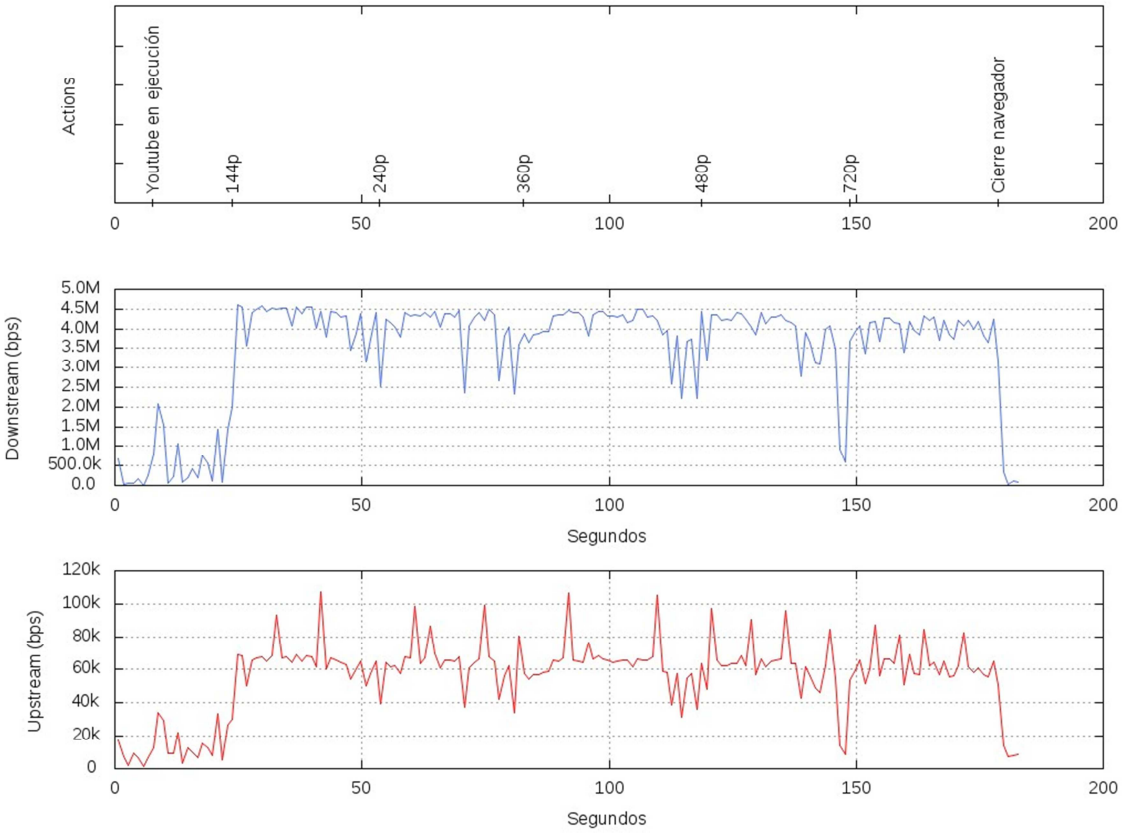

Figura 3.25. Perfil audiovisual sobre protocolo VNC limitado a 5 Mbps

Observamos como el protocolo está siendo limitado a la velocidad configurada sobre todas las calidades de vídeo.

La calidad de visualización de vídeos ya era bastante baja sin limitaciones, por ello, con este ancho de banda, la calidad sigue siendo muy mala.

3.2.1.3. TeamViewer

En el caso de TeamViewer, nunca llega a ocupar todo el ancho de la red. Por tanto, no llega a limitarse. Además, la calidad de vídeo en el perfil audiovisual sigue siendo bastante buena, sin llegar a existir cortes. Los datos extraídos están expuestos en la tabla comparativa posterior.

3.2.1.4. Tablas comparativas

A continuación, se muestra una tabla comparativa de los protocolos con cada uno de sus perfiles analizados, exponiendo su tasa media, tasa de pico y tasa total transferida en ambos sentidos, calculada sobre Excel mediante las funciones PROMEDIO, MÁX y SUMA, respectivamente.

Perfil	**Inicio de sesión**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	29 Kbps	44 Kbps	34 Kbps	7 Kbps	81 Kbps	76 Kbps
Tasa pico	106 Kbps	205 Kbps	277 Kbps	24 Kbps	220 Kbps	438 Kbps
Total (Bytes)	22 KB	33 KB	38 KB	8 KB	131 KB	123 KB
Calidad	5		5		5	
Perfil	**Ofimático**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	25 Kbps	6,5 Kbps	74 Kbps	6,3 Kbps	46 Kbps	12 Kbps
Tasa pico	250 Kbps	35 Kbps	842 Kbps	27,6 Kbps	311 Kbps	169 Kbps
Total (Bytes)	195 KB	50 KB	553 KB	47 KB	413 KB	109 KB
Calidad	5		5		5	

Perfil	Navegación					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	723 Kbps	16 Kbps	2,3 Mbps	39 Kbps	220 Kbps	9 Kbps
Tasa pico	4 Mbps	99 Kbps	5 Mbps	115 Kbps	1,6 Mbps	21 Kbps
Tasa total	14 MB	301 KB	44 MB	740 KB	4,7 MB	194 KB
Calidad	5		3		4	
Perfil	Audiovisual					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	4,25 Mbps	65 Kbps	3,5 Mbps	56 Kbps	900 Kbps	17 Kbps
Tasa pico	5 Mbps	189 Kbps	4,6 Mbps	107 Kbps	1,7 Mbps	175 Kbps
Tasa total	95 MB	1,4 MB	79 MB	1,3 MB	23 MB	425 KB
Calidad	4		1		4	

Tabla 2: Resultados con limitación a 5 Mbps

Combinaciones en las que la limitación está afectando notablemente

3.2.2. Limitación a 2 Mbps

3.2.2.1. RDP

En este protocolo, sobre esta limitación, empezamos a observar como el perfil de navegación se ve limitado. El perfil ofimático sigue sin hacerlo aunque sus movimientos empiezan a estar algo retardados. Sus estadísticas se observan en la tabla comparativa posterior.

- Perfil de navegación

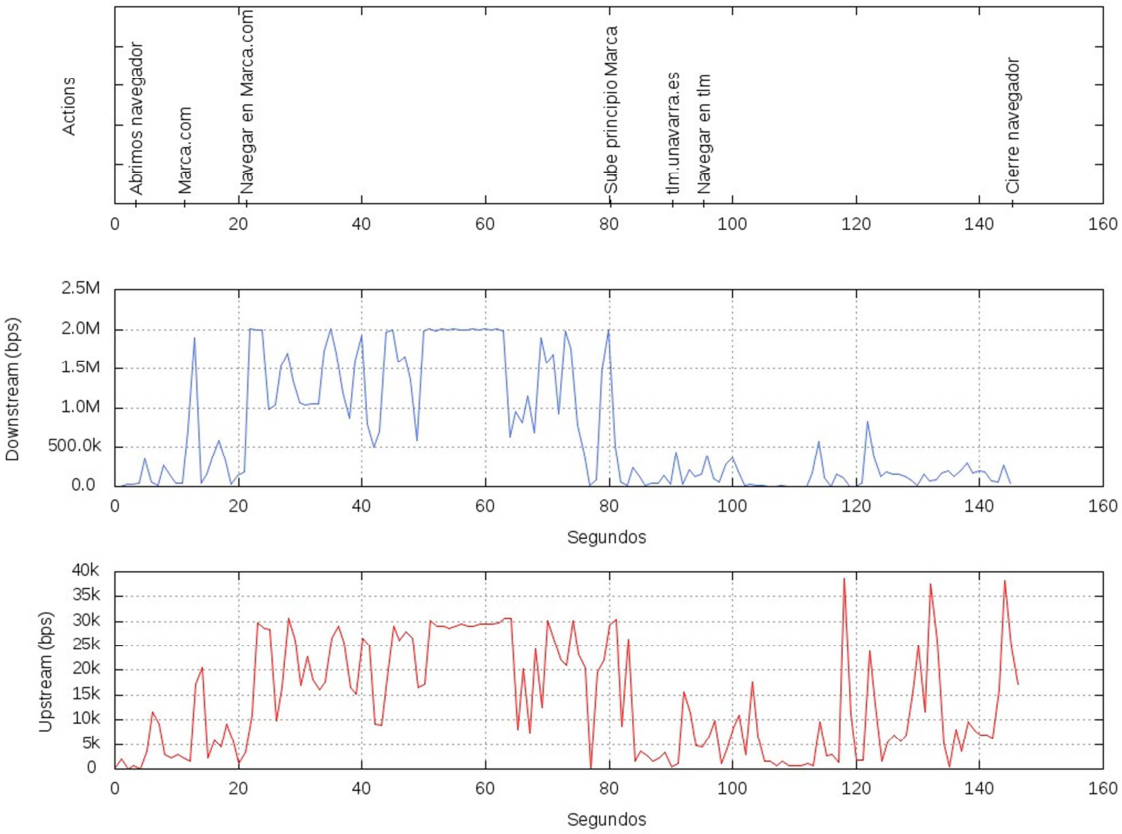

Figura 3.26. Perfil de navegación sobre protocolo RDP limitado a 2 Mbps

Este perfil se limita en la primera parte del análisis del perfil, cuando navega en la página de Marca. Además subjetivamente se nota en el scroll vertical cuando navegas sobre la página, ya que se nota el retardo.

- Perfil audiovisual

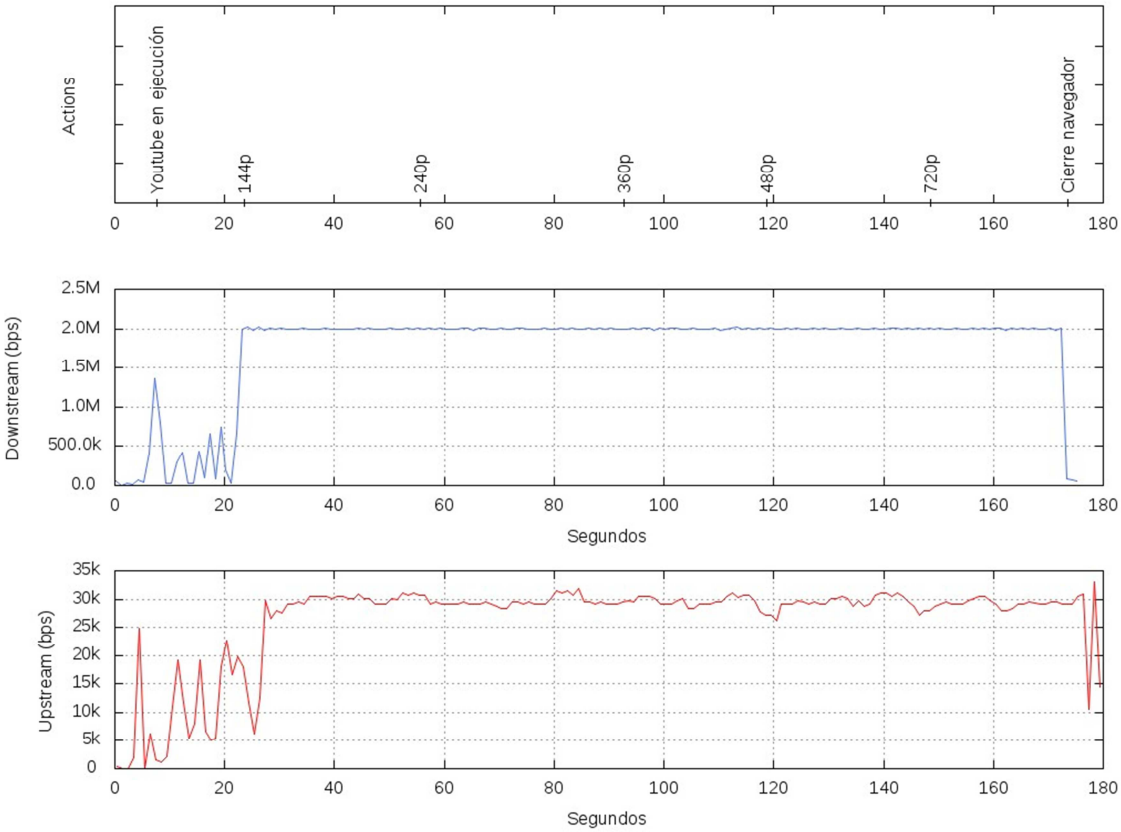

Figura 3.27. Perfil audiovisual sobre protocolo RDP limitado a 2 Mbps

Podemos observar como el perfil se limita a la velocidad configurada. La calidad va desmejorando, en casi todas las calidades de vídeo.

3.2.2.2. VNC

Sobre este protocolo se ve limitado tanto el perfil de navegación como el perfil audiovisual. El perfil ofimático se empieza a ver retardado en algunas acciones como el movimiento de ventana o el maximizado de ella. Sus valores estarán reflejados en la tabla comparativa posterior.

- Perfil de navegación

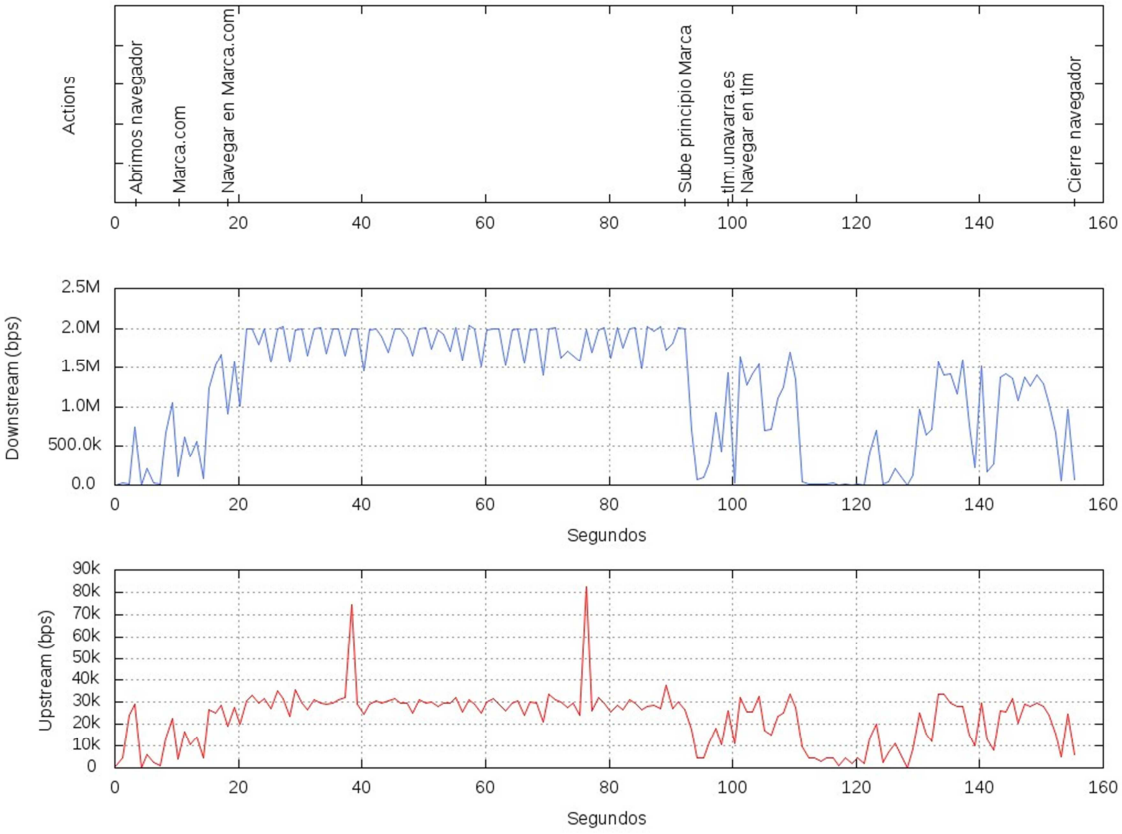

Figura 3.28. Perfil de navegación sobre protocolo VNC limitado a 2 Mbps

Como ocurre sobre RDP, navegar en la página de Marca se ve limitado a la velocidad configurada. El scroll también va retardado en su desplazamiento vertical.

- Perfil audiovisual

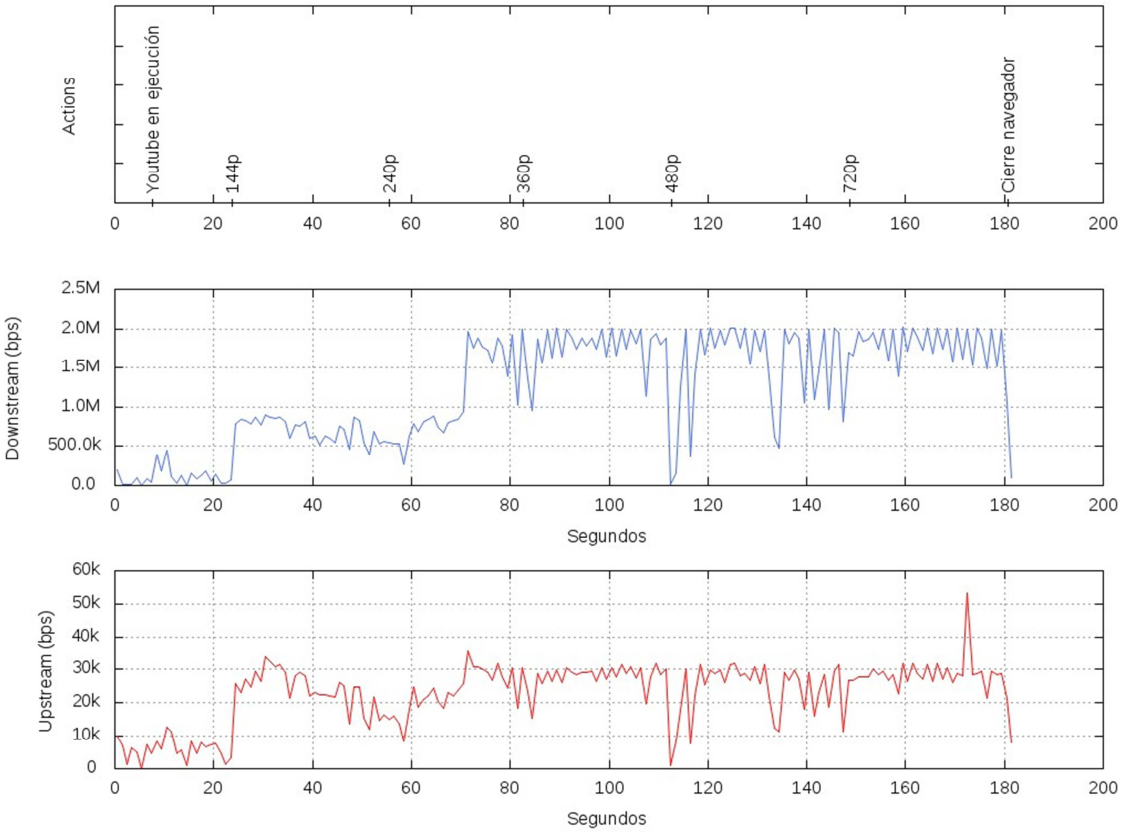

Figura 3.29. Perfil audiovisual sobre protocolo VNC limitado a 2 Mbps

En este perfil observamos como al aumentar la calidad del vídeo es cuando comienza a estar limitado éste. Como ocurre en todos los análisis sobre VNC del perfil audiovisual, la calidad de vídeo es muy baja.

3.2.2.3. TeamViewer

Como ocurría en la anterior configuración de limitación, esta configuración nunca llega a ocupar todo el ancho de la red. Por tanto, no llega a limitarse. Además, la calidad de vídeo en el perfil audiovisual sigue siendo buena, sin llegar a existir cortes. Los datos extraídos están expuestos en la tabla comparativa posterior.

3.2.2.4. Tablas comparativas

A continuación, se muestra una tabla comparativa de los protocolos con cada uno de sus perfiles analizados, exponiendo su tasa media, tasa de pico y tasa total transferida en ambos sentidos, calculada sobre Excel mediante las funciones PROMEDIO, MÁX y SUMA, respectivamente.

Perfil	**Inicio de sesión**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	33 Kbps	44 Kbps	30,5 Kbps	7 Kbps	56 Kbps	69 Kbps
Tasa pico	131 Kbps	203 Kbps	225 Kbps	32 Kbps	220 Kbps	541 Kbps
Total (Bytes)	25 KB	33 KB	38 KB	9 KB	99 KB	121 KB
Calidad	5		4		4	
Perfil	**Ofimático**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	16 Kbps	7 Kbps	127 Kbps	7 Kbps	110 Kbps	14 Kbps
Tasa pico	69 Kbps	35 Kbps	690 Kbps	18 Kbps	1,6 Mbps	171 Kbps
Total (Bytes)	118 KB	50 KB	997 KB	55 KB	910 KB	115 KB
Calidad	4		4		4	

Perfil	Navegación					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	692 Kbps	14 Kbps	1,2 Mbps	23 Kbps	250 Kbps	14 Kbps
Tasa pico	2 Mbps	39 Kbps	2 Mbps	82 Kbps	1,5 Mbps	176 Kbps
Tasa total	12,5 MB	257 KB	24 MB	445 KB	5,2 MB	283 KB
Calidad	4		3		3	
Perfil	Audiovisual					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	1,7 Mbps	26 Kbps	1,2 Mbps	23 Kbps	606 Kbps	20 Kbps
Tasa pico	2 Mbps	33 Kbps	2 Mbps	53 Kbps	2 Mbps	195 Kbps
Tasa total	38 MB	593 KB	28 MB	523 KB	15 MB	490 KB
Calidad	3		1		3	

Tabla 3: Resultados con limitación a 2 Mbps

Combinaciones en las que la limitación está afectando notablemente

3.2.3. Limitación a 1 Mbps

3.2.3.1. RDP

Sobre esta limitación, aunque el perfil ofimático no llegue al ancho de banda establecido, sí que se ve afectado en las acciones que se realizan sobre este perfil. Sus valores estarán reflejados en la tabla comparativa posterior.

Los otros dos perfiles sí se ven limitados y disminuyen notablemente la calidad de sus acciones. Aquí mostramos sus gráficas:

- Perfil de navegación

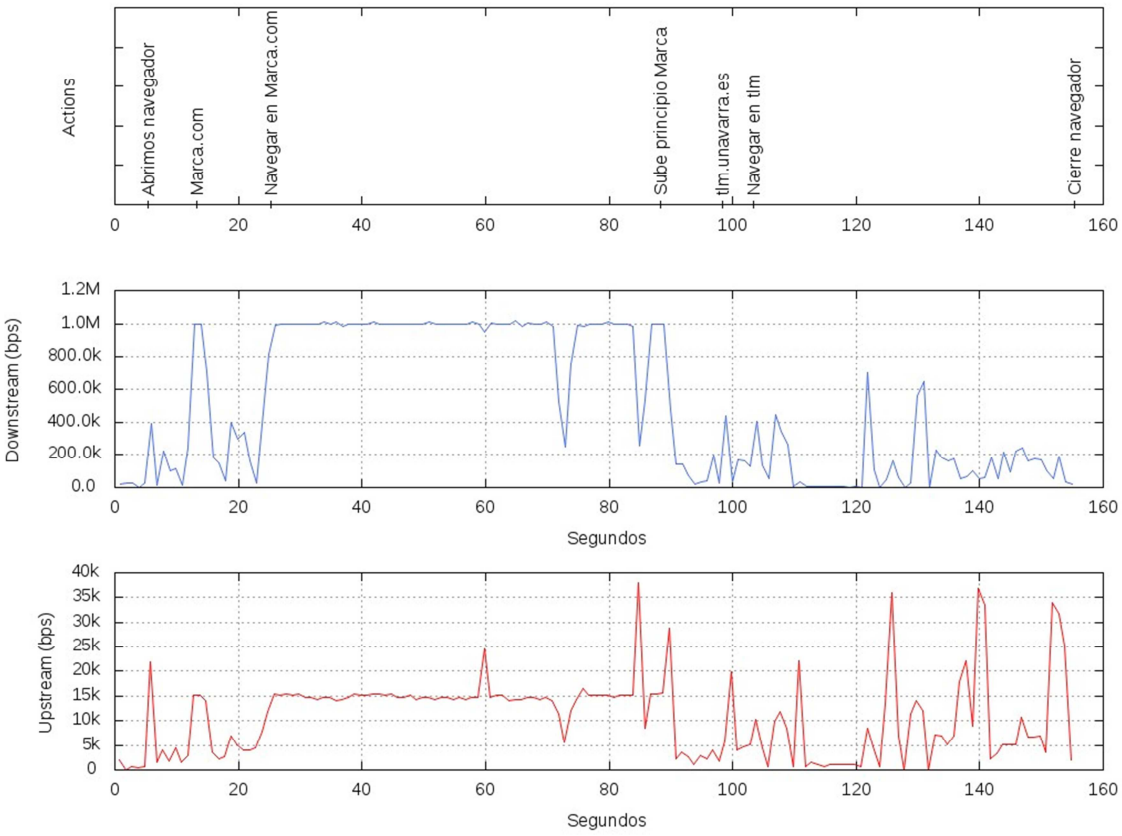

Figura 3.30. Perfil de navegación sobre protocolo RDP limitado a 1 Mbps

- Perfil audiovisual

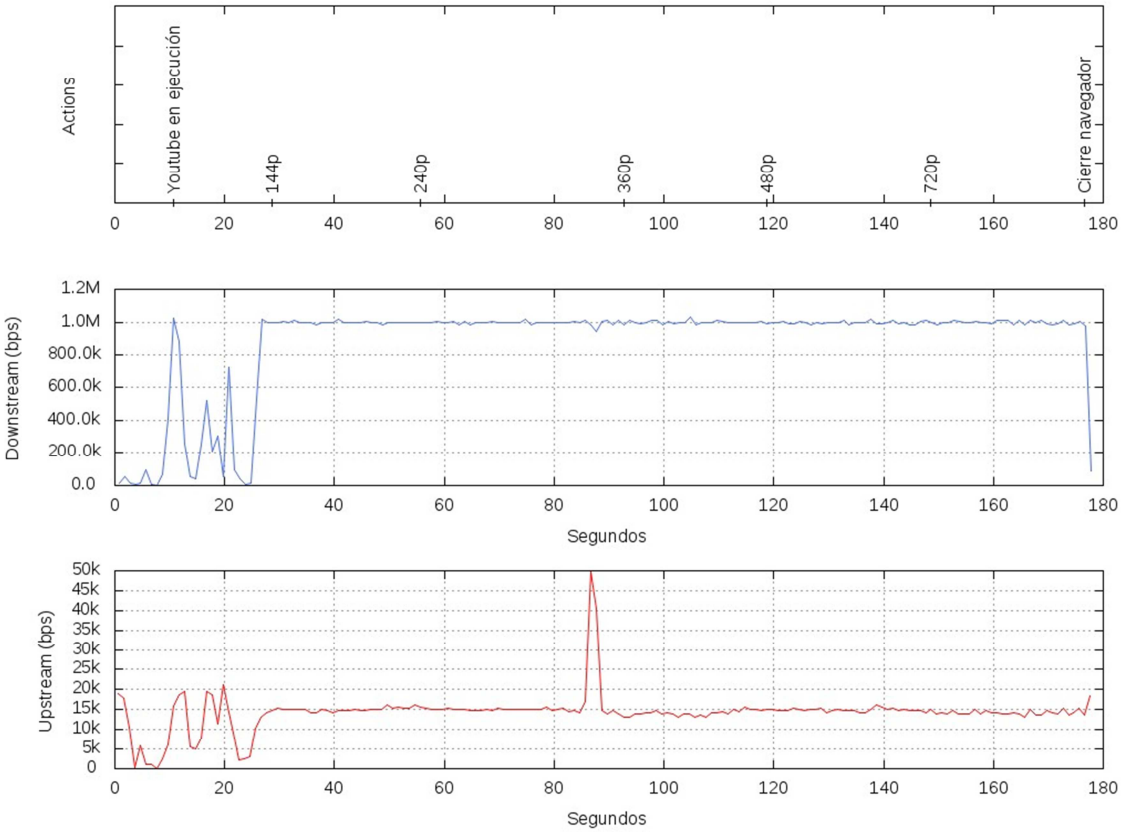

Figura 3.31. Perfil audiovisual sobre protocolo RDP limitado a 1 Mbps

3.2.3.2. VNC

Sobre esta limitación, como ocurre en RDP, el perfil ofimático no llega al ancho de banda configurado pero si se ve afectado. Los otros perfiles si se limitan y las gráficas son las siguientes:

- Perfil de navegación

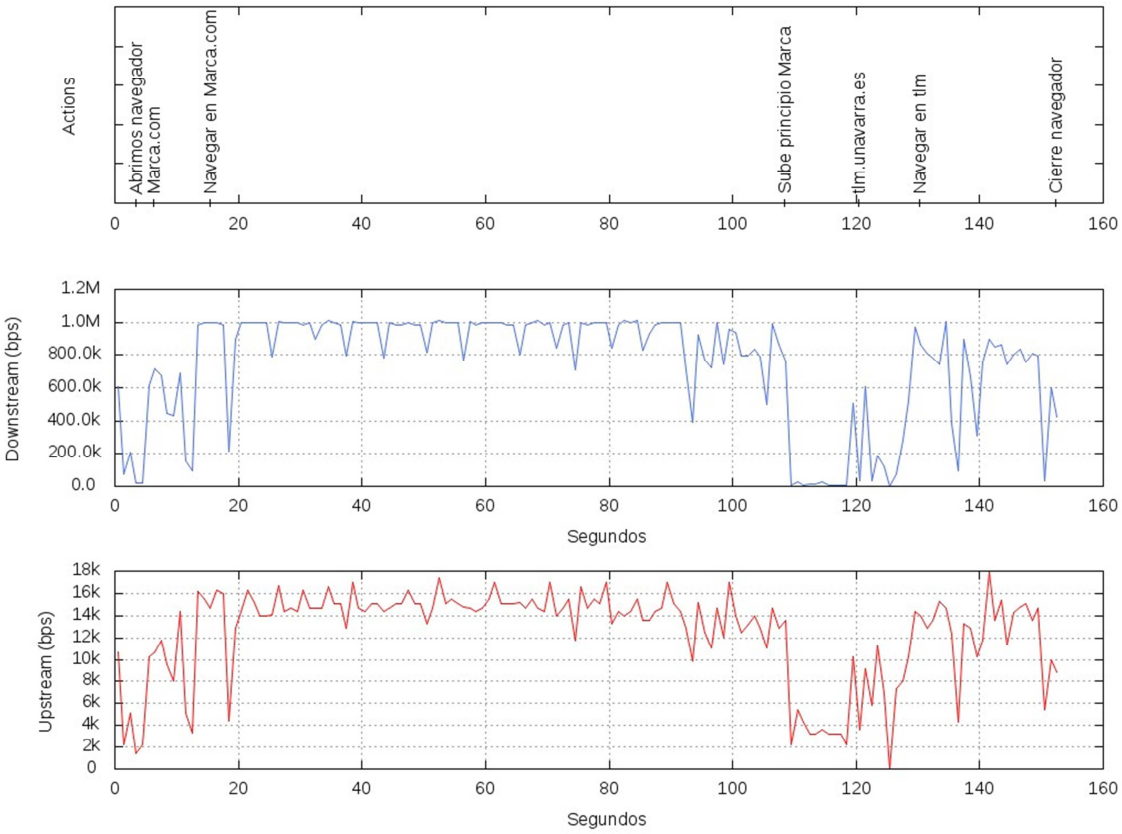

Figura 3.32. Perfil de navegación sobre protocolo VNC limitado a 1 Mbps

Observamos cómo incluso en el momento de navegar por el área de telemática, hay picos de ancho de banda limitándose a 1 Mbps.

- Perfil audiovisual

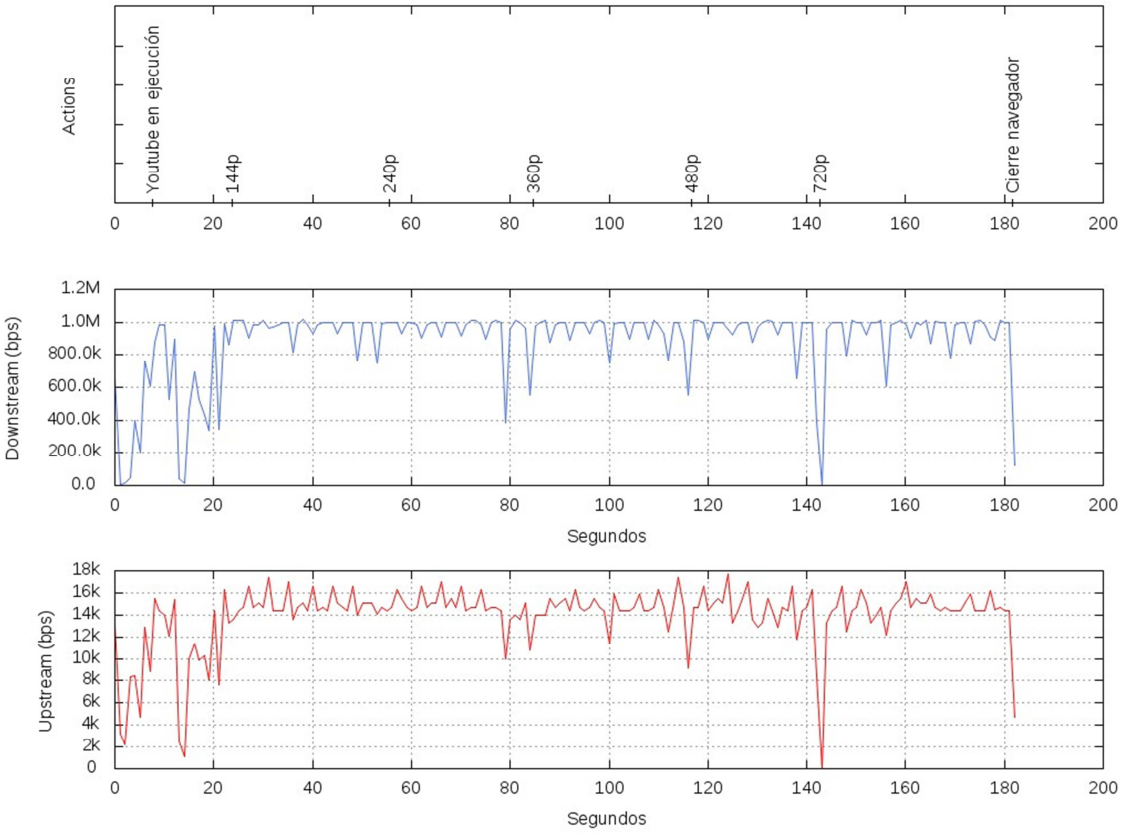

Figura 3.33. Perfil audiovisual sobre protocolo VNC limitado a 1 Mbps

3.2.3.3. TeamViewer

Sobre TeamViewer limitado a 1 Mbps, podemos encontrar limitaciones en el perfil de navegación y en el perfil audiovisual. Sobre el perfil ofimático se observarán sus resultados en la tabla comparativa posterior.

- Perfil de navegación

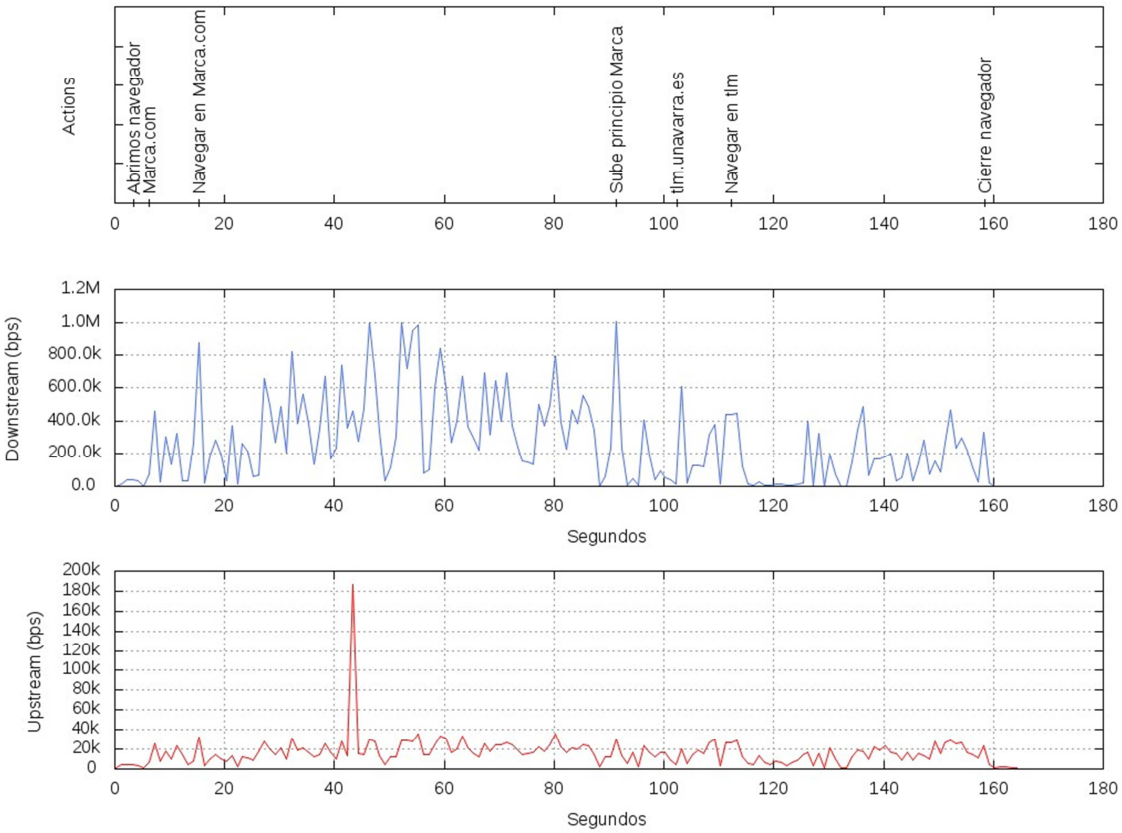

Figura 3.34. Perfil de navegación sobre TeamViewer limitado a 1 Mbps

Navegando sobre Marca observamos picos de ancho de banda a la velocidad limitada.

- Perfil audiovisual

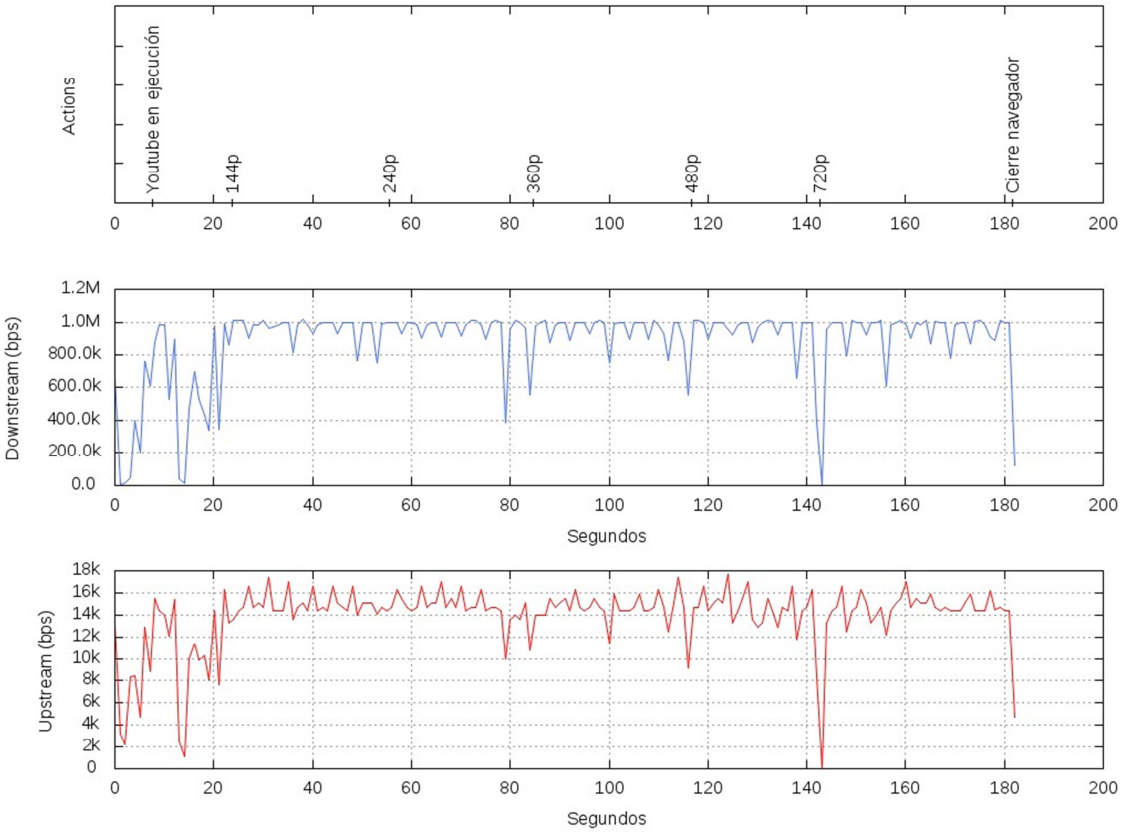

Figura 3.35. Perfil audiovisual sobre TeamViewer limitado a 1 Mbps

3.2.3.4. Tablas comparativas

A continuación, se muestra una tabla comparativa de los protocolos con cada uno de sus perfiles analizados, exponiendo su tasa media, tasa de pico y tasa total transferida en ambos sentidos, calculada sobre Excel mediante las funciones PROMEDIO, MÁX y SUMA, respectivamente.

Perfil	**Inicio de sesión**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	31 Kbps	44 Kbps	27 Kbps	6 Kbps	55 Kbps	68 Kbps
Tasa pico	111 Kbps	200 Kbps	277 Kbps	37 Kbps	233 Kbps	456 Kbps
Total (Bytes)	23 KB	33 KB	44 KB	10 KB	97 KB	120 KB
Calidad	4		3		3	
Perfil	**Ofimático**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	25 Kbps	6,4 Kbps	93 Kbps	6,2 Kbps	69 Kbps	14 Kbps
Tasa pico	227 Kbps	37,8 Kbps	600 Kbps	15,6 Kbps	500 Kbps	183 Kbps
Total (Bytes)	193 KB	50 KB	733 KB	48 KB	564 KB	114 KB
Calidad	3		2		3	

Perfil	Navegación					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	496 Kbps	11 Kbps	738 Kbps	12,4 Kbps	263 Kbps	17 Kbps
Tasa pico	1 Mbps	38 Kbps	1 Mbps	18 Kbps	1 Mbps	186,5 Kbps
Tasa total	9,6 MB	209 KB	14 MB	238 KB	5,4 MB	345 KB
Calidad	3		2		3	
Perfil	Audiovisual					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	878 Kbps	14 Kbps	887 Kbps	14 Kbps	371,5 Kbps	19,7 Kbps
Tasa pico	1 Mbps	50 Kbps	1 Mbps	18 Kbps	1 Mbps	190 Kbps
Tasa total	19,5 MB	319 KB	20,2 MB	319 KB	9,2 MB	490 KB
Calidad	2		1		3	

Tabla 4: Resultados con limitación a 1 Mbps

	Combinaciones en las que la limitación está afectando notablemente

3.2.4. Limitación a 300 Kbps

Con esta limitación pretendemos comprobar cómo funcionan los diferentes perfiles en entornos de muy bajo ancho de banda, como podría ser en una conexión vía Smartphone o Tablet.

3.2.4.1. RDP

Aquí mostraremos los tres perfiles, aunque el perfil ofimático no llegue a limitar, sí que sufre grandes retardos en movimientos de ventana, o apertura de carpetas.

- Perfil ofimático

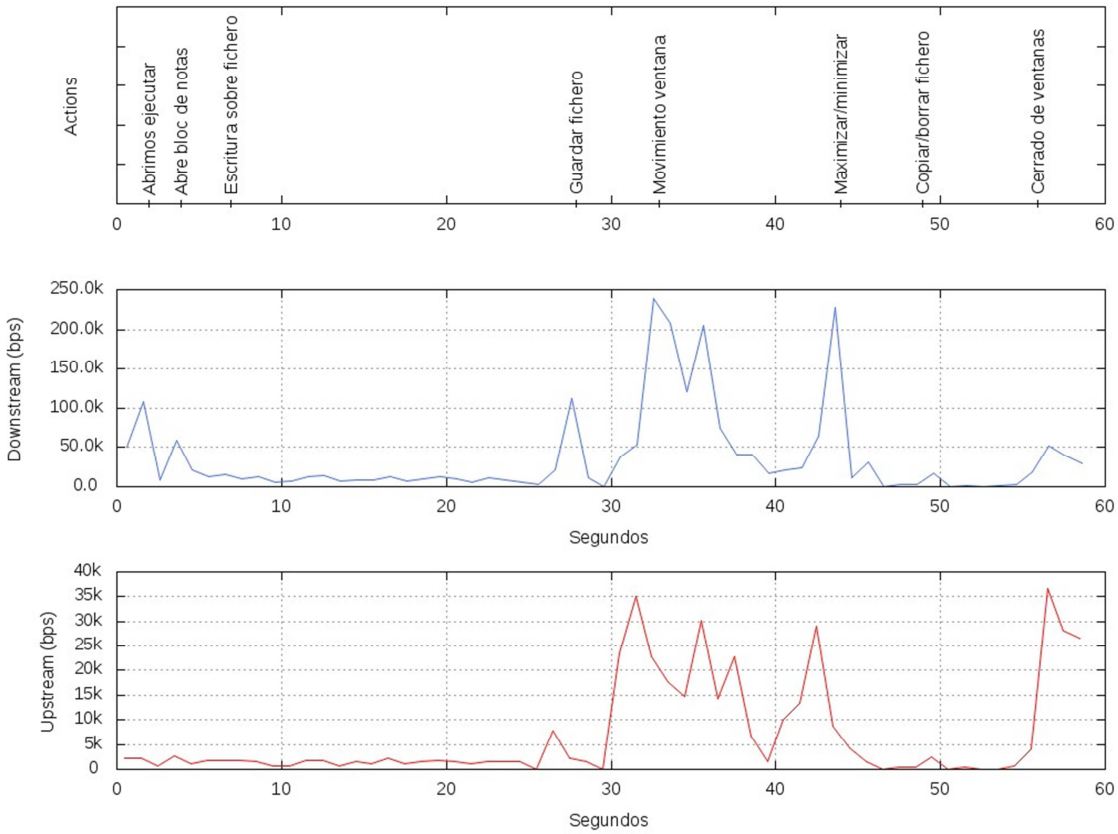

Figura 3.36. Perfil ofimático sobre protocolo RDP limitado a 300 Kbps

- Perfil de navegación

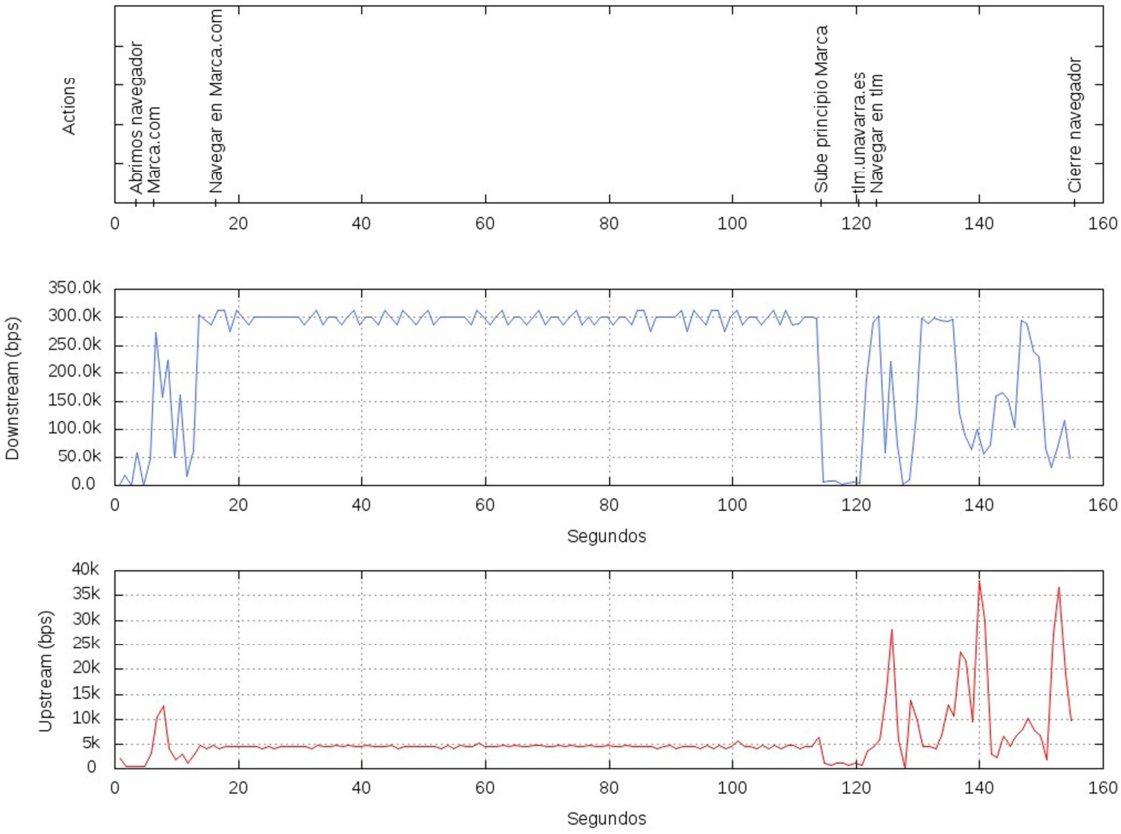

Figura 3.37. Perfil de navegación sobre protocolo RDP limitado a 300 Kbps

Está limitado a 300 Kbps prácticamente en toda la macro grabada sobre perfil de navegación.

- Perfil audiovisual

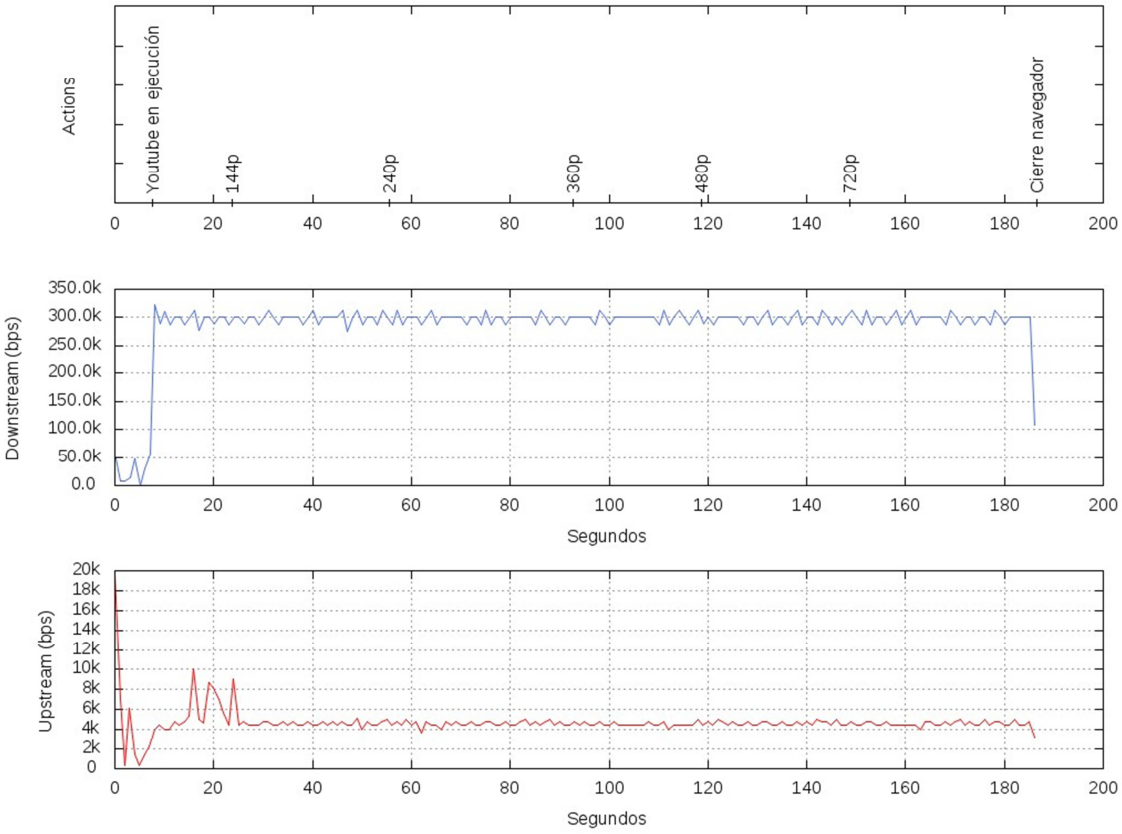

Figura 3.38. Perfil audiovisual sobre protocolo RDP limitado a 300 Kbps

3.2.4.2. VNC

Aquí observamos los diferentes resultados sobre este protocolo limitado a 300 Kbps.

- Perfil ofimático

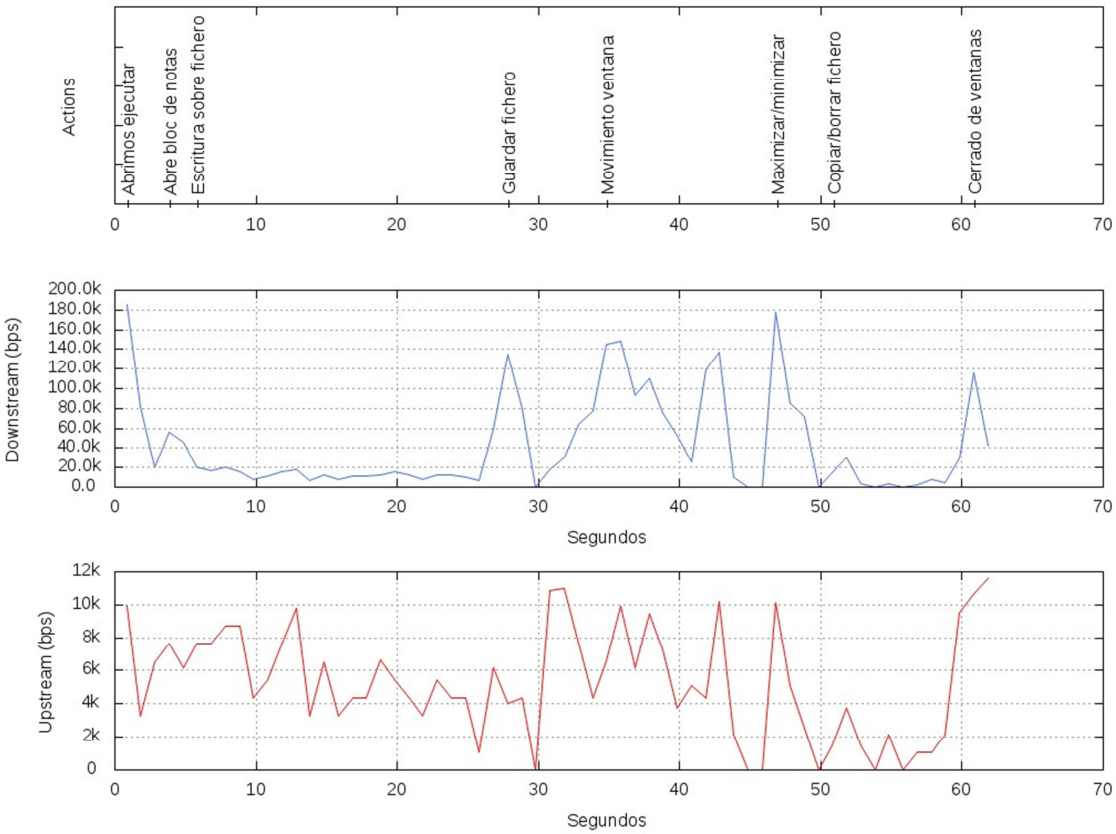

Figura 3.39. Perfil ofimático sobre protocolo VNC limitado a 300 Kbps

No llega a la limitación configurada pero si se nota un desmejoramiento del perfil notable. En la tabla posterior se verán los resultados.

- Perfil de navegación

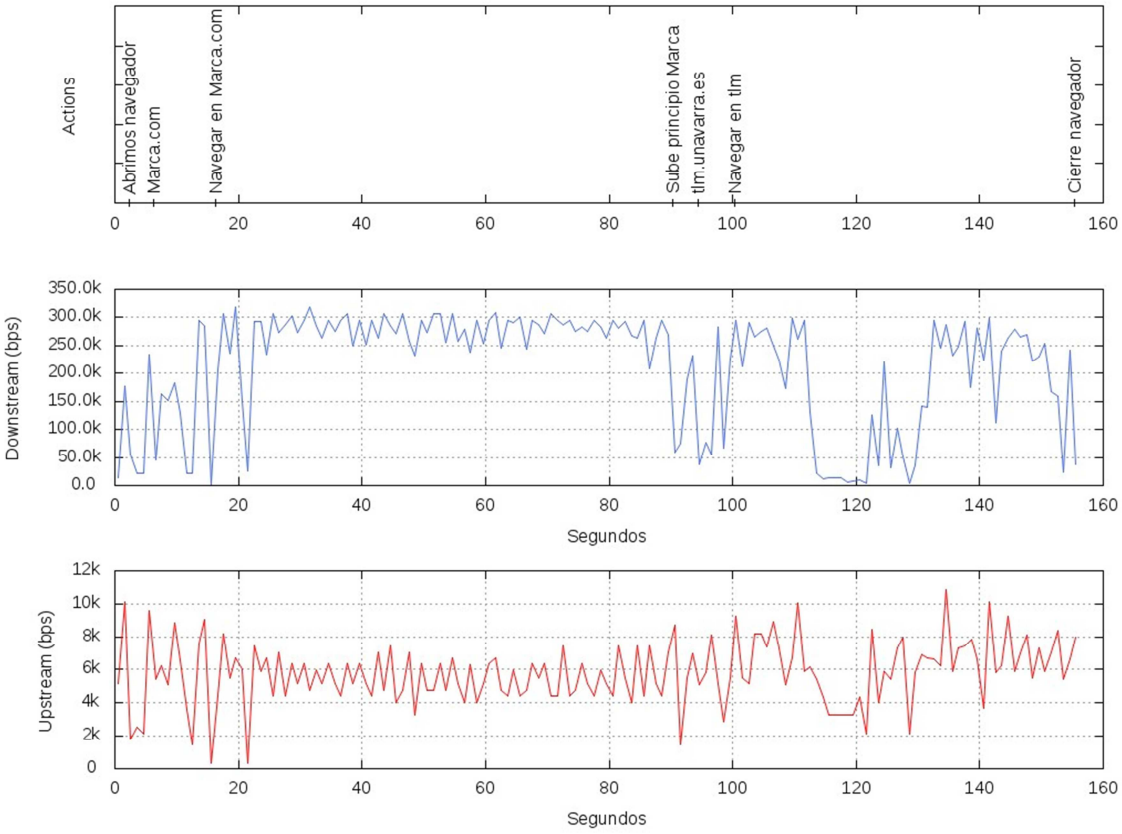

Figura 3.40. Perfil de navegación sobre protocolo VNC limitado a 300 Kbps

- Perfil audiovisual

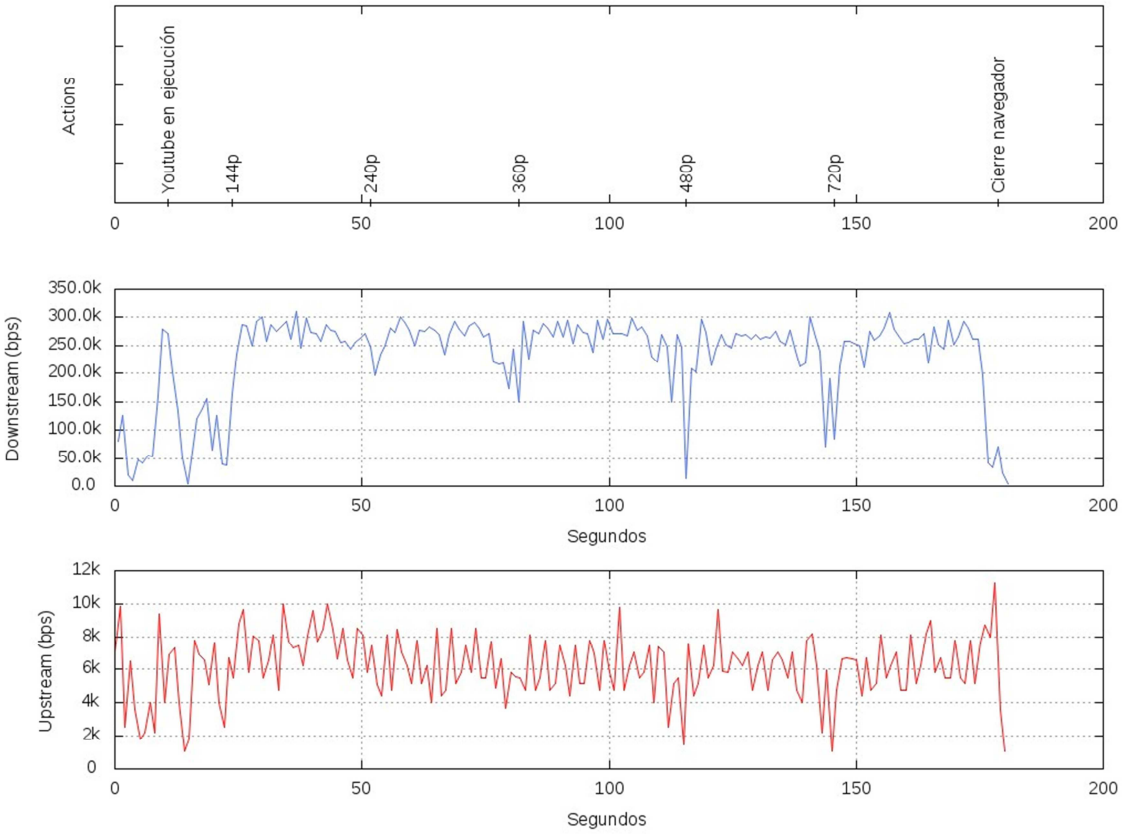

Figura 3.41. Perfil audiovisual sobre protocolo VNC limitado a 300 Kbps

3.2.4.3. TeamViewer

- Perfil ofimático

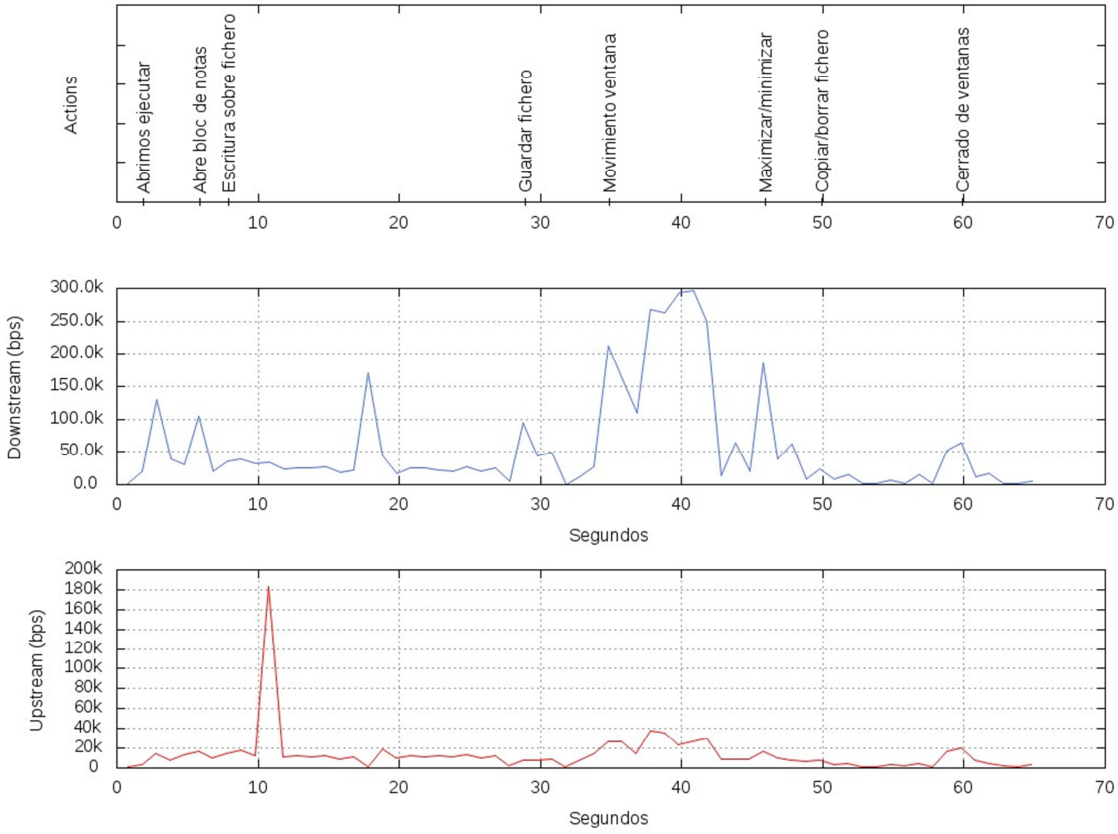

Figura 3.42. Perfil ofimático sobre TeamViewer limitado a 300 Kbps

- Perfil de navegación

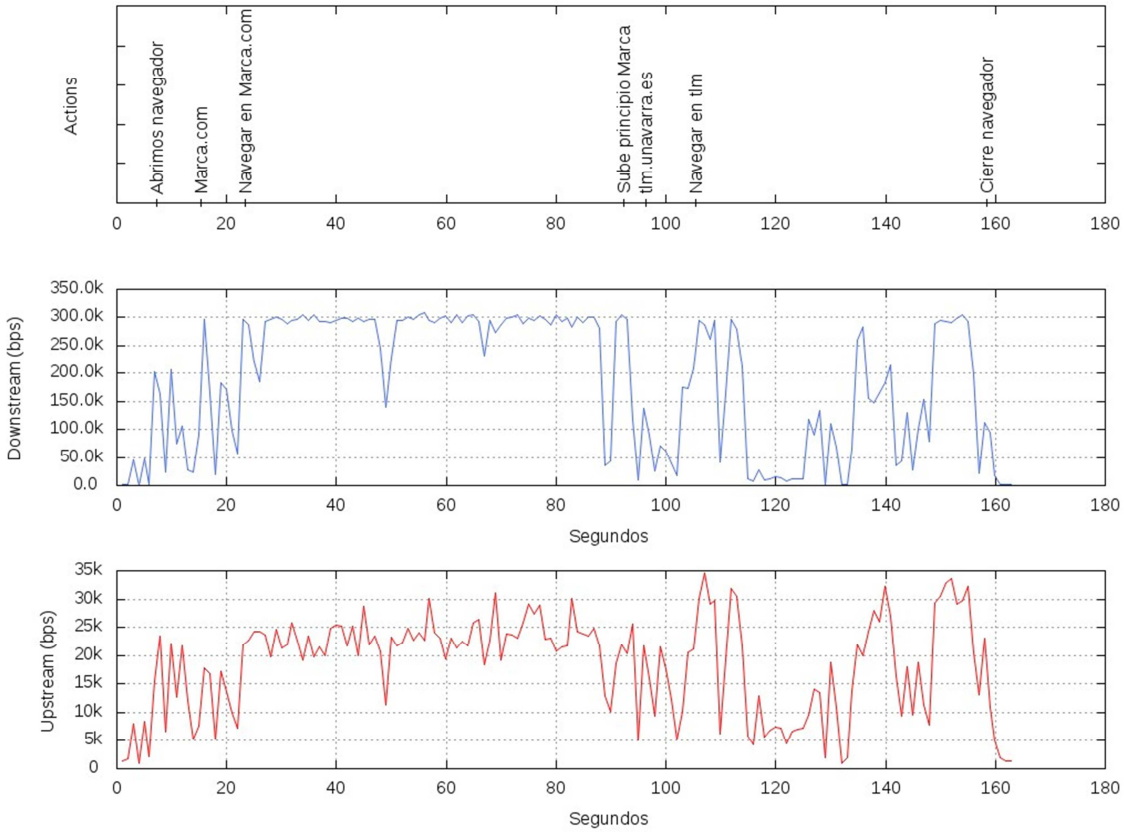

Figura 3.43. Perfil de navegación sobre TeamViewer limitado a 300 Kbps

- Perfil audiovisual

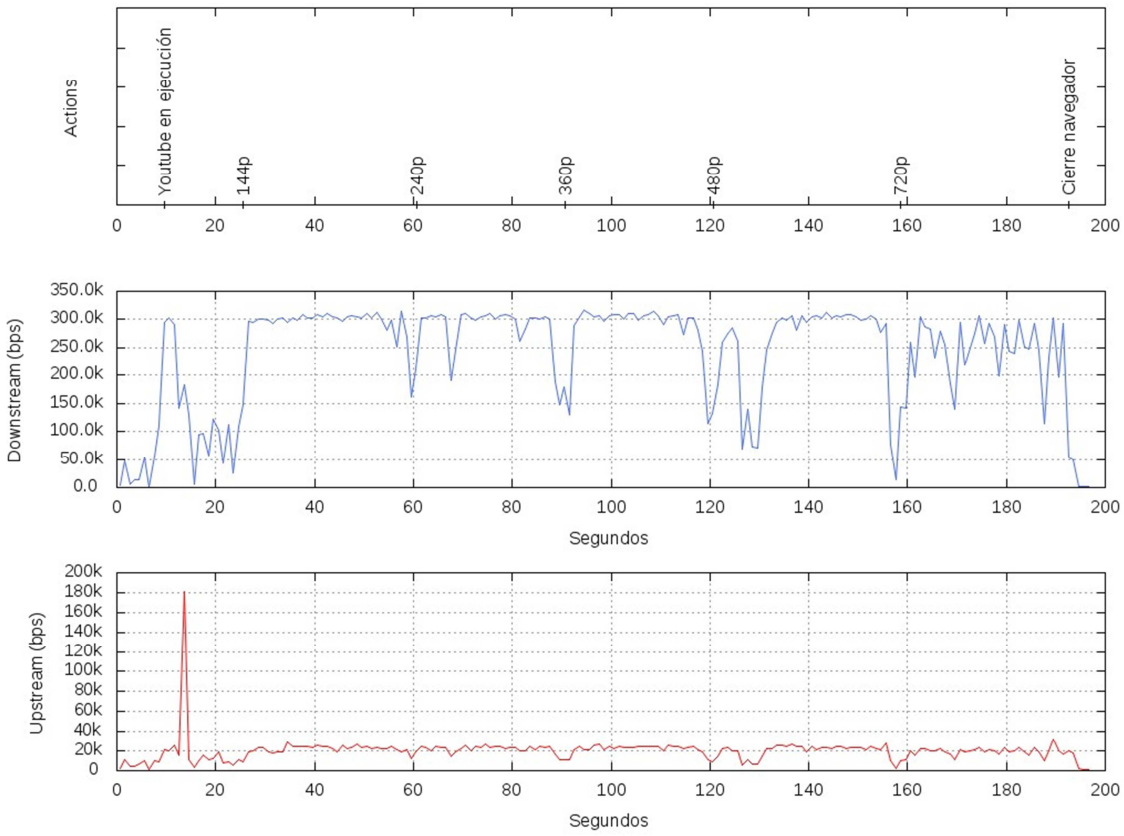

Figura 3.44. Perfil audiovisual sobre TeamViewer limitado a 300 Kbps

3.2.4.4. Tablas comparativas

A continuación, se muestra una tabla comparativa de los protocolos con cada uno de sus perfiles analizados, exponiendo su tasa media, tasa de pico y tasa total transferida en ambos sentidos, calculada sobre Excel mediante las funciones PROMEDIO, MÁX y SUMA, respectivamente.

Perfil	**Inicio de sesión**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	29 Kbps	44 Kbps	44 Kbps	7,6 Kbps	46 Kbps	74 Kbps
Tasa pico	88 Kbps	199 Kbps	257 Kbps	28,8 Kbps	178 Kbps	461 Kbps
Total (Bytes)	22 KB	33 KB	72 KB	12 KB	75 KB	120 KB
Calidad	3		2		3	
Perfil	**Ofimático**					
	RDP		**VNC**		**TeamViewer**	
	Downstream	**Upstream**	**Downstream**	**Upstream**	**Downstream**	**Upstream**
Tasa media	37 Kbps	7 Kbps	42 Kbps	5,3 Kbps	57 Kbps	14 Kbps
Tasa pico	240 Kbps	36,7 Kbps	195 Kbps	11,6 Kbps	300 Kbps	183 Kbps
Total (Bytes)	272 KB	50,7 KB	329 KB	40,7 KB	466 KB	113 KB
Calidad	3		2		3	

Perfil	Navegación					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	237 Kbps	5,8 Kbps	219 Kbps	5,8 Kbps	187 Kbps	18,4 Kbps
Tasa pico	300 Kbps	38 Kbps	300 Kbps	11 Kbps	300 Kbps	34,5 Kbps
Tasa total	4,6 MB	113 KB	4,1 MB	113 KB	3,8 MB	375 KB
Calidad	3		1		3	
Perfil	**Audiovisual**					
	RDP		VNC		TeamViewer	
	Downstream	Upstream	Downstream	Upstream	Downstream	Upstream
Tasa media	285,6 Kbps	4,7 Kbps	230 Kbps	6 Kbps	241,5 Kbps	20,3 Kbps
Tasa pico	300 Kbps	19,7 Kbps	300 Kbps	11 Kbps	300 Kbps	181 Kbps
Tasa total	6,7 MB	109,6 KB	5,2 MB	140 KB	6 MB	500 KB
Calidad	1		1		2	

Tabla 5: Resultados con limitación a 300 Kbps

Combinaciones en las que la limitación está afectando notablemente

4. Conclusiones

Ante los resultados obtenidos sobre las distintas limitaciones y sus tasas obtenidas en cada uno de los perfiles, aquí mostramos una tabla resumen de las calidades obtenidas:

		Calidad		
		RDP	**VNC**	**TeamViewer**
Sin limitación	**Inicio sesión**	5	5	5
	Ofimático	5	5	5
	Navegación	5	4	4
	Audiovisual	5	1	4
5 Mbps	**Inicio sesión**	5	5	5
	Ofimático	5	5	5
	Navegación	5	3	4
	Audiovisual	4	1	4
2 Mbps	**Inicio sesión**	5	4	4
	Ofimático	4	4	4
	Navegación	4	3	3
	Audiovisual	3	1	3
1 Mbps	**Inicio sesión**	4	3	3
	Ofimático	3	2	3
	Navegación	3	2	3
	Audiovisual	3	1	3
300 Kbps	**Inicio sesión**	3	2	3
	Ofimático	3	2	3
	Navegación	3	1	3
	Audiovisual	1	1	2

Tabla 6: Resultados de calidad

Como observamos, cuando nos encontramos en un entorno donde el ancho de banda es muy grande, no tenemos prácticamente ningún inconveniente para ningún protocolo a excepción de ver vídeos con VNC, el cuál cómo ya se comentó, es muy bajo de calidad, con paradas de vídeo, muy píxelado e imposible de visualizar.

También observamos como TeamViewer es el más estable incluso en anchos de banda muy bajos, como puede ser conexiones a través de Tablets o Smartphones. Por ello, creemos que es el mejor para entornos de este tipo ya que incluso es capaz de visualizar un vídeo medianamente bien en calidad baja, aunque exista una calidad muy píxelada y a veces el vídeo sufra pequeños cortes debido a grandes movimientos en el contenido del vídeo.

Además, recalcar el bajón que provoca el protocolo RDP una vez comienza a tener serias limitaciones, desde un perfil de inicio de sesión hasta el perfil audiovisual. Creemos que este protocolo solo es recomendable en entornos con un ancho de banda mayor de 2-5 Mbps.

Sobre el protocolo VNC podemos concluir que es un protocolo muy básico, con muchas limitaciones en entornos audiovisuales, pero factible en muchos entornos de utilización del escritorio remoto para aplicaciones ofimáticas o de navegación en un ancho de banda notable (a partir de 5 Mbps).

Por ello creemos que tanto el protocolo RDP como el protocolo VNC están un poco por debajo de las expectativas que nos ofrece TeamViewer en casi todos los entornos analizados, pero también esperamos que en el futuro ambos protocolos vayan en auge y mejoren sus prestaciones para dar a sus clientes grandes satisfacciones y, sobre todo, ayuden a mejorar a las empresas para poder utilizar los escritorios gestionados en la nube de la mejor forma que sea posible. Además los tres protocolos analizados actualmente están disponibles como aplicaciones Android para acceder a los equipos informáticos a través de tu Smartphone o de tu Tablet.

Con el protocolo VNC está VNC Viewer [24], con el protocolo RDP encontramos Microsoft Remote Desktop [25] y por último, TeamViewer [26].

Referencias

[1] Foro La Pipa Plena. *Configurar un server para compartir Internet a modo Router.* Marzo 2012. URL: http://www.lapipaplena.net/foro/index.php?topic=40.0

[2] The Dark Phiside. *Configurar dos tarjetas de red en Ubuntu.* Mayo 2013. URL: https://wdb.ugr.es/~amaro/darkphyside/thema.php?board=9&thema=5

[3] Ubuntu. *Problema con DNS Ubuntu Server.* Marzo 2011. URL: http://www.ubuntu-es.org/node/151504#.Vu2eH-LhDIW

[4] Manual Ubuntu. *Manipulate traffic control settings.* URL: http://manpages.ubuntu.com/manpages/trusty/man8/tc.8.html

[5] Manual Ubuntu. *NetEm, Network Emulator.* URL: http://manpages.ubuntu.com/manpages/trusty/man8/tc-netem.8.html

[6] LARTC. *Rate limiting a single host or netmask*. URL: http://lartc.org/howto/lartc.ratelimit.single.html

[7] Amazon Web Services. *Cloud Computing – Servicios de informática en la nube*. URL: https://aws.amazon.com/es/?nc2=h_lg

[8] Macro Recorder. URL: https://www.jitbit.com/macro-recorder/

[9] Tutorial sobre GNUPlot. URL: https://freeshell.de/~rgh/arch/gnuplot-tut.pdf

[10] Manual tcpstat. URL: http://linux.die.net/man/1/tcpstat

[11] Manual n2n. URL: http://linux.die.net/man/8/edge

[12] Tutoriales fáciles. *Montar servidor FTP con Filezilla Server*. URL: https://tutorialesfaciles.wordpress.com/windows/montar-servidor-ftp-con-filezilla-server/

[13] Redes Zone. *SSH Tunneling*. URL: http://www.redeszone.net/redes/ssh-tunneling/

[14] Culturación. *Qué es y para qué sirve el escritorio remoto*. URL: http://culturacion.com/que-es-escritorio-remoto/

[15] Microsoft. *Descripción del protocolo de escritorio remoto (RDP).* URL: https://support.microsoft.com/es-es/kb/186607

[16] Impoweru. *Requisitos VNC de ancho de banda.* URL: http://www.impoweru.com/requisitos-vnc-de-ancho-de-banda/

[17] Wikipedia. *Protocolo RDP*. URL: https://es.wikipedia.org/wiki/Remote_Desktop_Protocol

[18] Universidad Técnica Federico Santa María. *Informe "Escritorio remoto".* URL: http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/EscritorioRemoto.pdf

[19] Wikipedia. *Protocolo VNC*. URL: https://es.wikipedia.org/wiki/VNC

[20] TeamViewer. URL: https://www.teamviewer.com/es/

[21] Wikipedia. *Run Length Encoding*. URL: https://es.wikipedia.org/wiki/Run-length_encoding

[22] Wikipedia. *JPEG*. URL: https://en.wikipedia.org/wiki/JPEG

[23] Stack Overflow. *Foro de múltiples ayudas*. URL: http://stackoverflow.com/

[24] Play Google. *VNC Viewer*. URL: https://play.google.com/store/apps/details?id=com.realvnc.viewer.android

[25] Play Google. Microsoft Remote Desktop. URL: https://play.google.com/store/apps/details?id=com.microsoft.rdc.android

[26] Play Google. TeamViewer: URL: https://play.google.com/store/apps/details?id=com.teamviewer.teamviewer.market.mobile

Anexos

Anexo 1: Script tcpstat.sh

```
#!/bin/sh

## Argumentos de entrada:
## 1-Nombre de la captura
## 2-Nombre para los datos de bajada
## 3-Nombre para los datos de subida
tcpstat -r $1.pcap 1 -f 'src (52.29.252.161)' -o "%s\t%b\n" > $2.data

tcpstat -r $1.pcap 1 -f 'dst (52.29.252.161)' -o "%s\t%b\n" > $3.data

## -r -> Introducimos el fichero de captura
## 1 -> Obtener los datos en intervalos de un segundo
## -f -> Filtramos por IP origen o destino
## -o -> Sacamos como valores, el tiempo UNIX y los bps
## > .data -> Sacar un fichero .data con los valores obtenidos
```

Anexo 2: Script plot.sh

```
#!/bin/sh

## Argumentos de entrada:
## 1-Nombre del fichero data de bajada
## 2-Nombre del fichero data de subida
## 3-Nombre del fichero de etiquetas
## 4-Nombre de la gráfica resultante

gnuplot << EOF
set terminal jpeg size 1024,768
set output "$4.jpg"
set multiplot layout 3,1
set lmargin 10
set bmargin 3

set yrange [0:5]
set ylabel "Actions"
set format y " "
unset key
plot '$3.data' using 1:2:3 with labels point tc rgb "black" rotate left

set yrange [0:*]
set xlabel "Segundos"
set ylabel "Downstream (bps)"
set format y "%.1s%c"
unset key
set grid
plot "$1.data" lt 8 w l

set yrange [0:*]
set xlabel "Segundos"
set ylabel "Upstream (bps)"
set format y "%.0s%c"
unset key
set grid
plot "$2.data" w l
unset multiplot


EOF
## set terminal -> Formato del archivo resultante
## set output -> Archivo de imagen resultante
## set multiplot -> Formato del multiplot, con tres gráficas en una
columna
## set lmargin y bmargin -> Márgenes de alrededor del gráfico
## set yrange -> Rango de valores entre los que estarán los resultados
obtenidos
## set ylabel -> Etiquetas para el eje Y
## unset key -> Eliminar los ejes
## plot '$3.data' using 1:2:3 with labels point tc rgb "black" rotate
left -> Pintado de las etiquetas, en color negro y en vertical
## set format y "%.1s%c" -> Formato del eje Y en notación de
ingeniería
## plot "$1.data" lt 8 w l -> Pintado del downstream de color azul
## plot "$2.data" w l -> Pintado del up stream de color rojo
## unset multiplot -> Fin del multiplot
```

Anexo 3: Script shaper.sh

```
#!/bin/sh

# Parametros a introducir:
# 1-status, stop o start, según la opción que se desee
# 2-interfaz el cual queremos añadir la limitación
# 3-velocidad a la que se quiere limitar

DEV=$2

if [ "$1" = "status" ]
then
    # Observamos la configuración establecida
    tc -s qdisc ls dev $DEV
    tc -s class ls dev $DEV
    exit
fi

if [ "$1" = "stop" ]
then
    # Eliminamos configuraciones establecidas
    tc qdisc del dev $DEV root    2> /dev/null > /dev/null
    tc qdisc del dev $DEV ingress 2> /dev/null > /dev/null
    exit
fi

if [ "$1" = "start" ]
then

    RATE=$3
    # Eliminamos cualquier configuración anterior si la hubiese
    tc qdisc del dev $DEV root    2> /dev/null > /dev/null
    tc qdisc del dev $DEV ingress 2> /dev/null > /dev/null

    # Crear root CBQ
    tc qdisc add dev $DEV root handle 1: cbq avpkt 1000 bandwidth
10mbit

    # Creamos la clase principal
    tc class add dev $DEV parent 1: classid 1:1 cbq rate ${RATE}kbit
allot 1500 prio 5 bounded isolated

    # Filtramos para cualquier IP destino
    tc filter add dev $DEV parent 1: protocol ip prio 18 u32 match ip
dst 0.0.0.0/0 flowid 1:1
fi
```